

Troubleshooting Routers

BayRS Version 12.00
Site Manager Software Version 6.00

Part No. 117379-A Rev. A
September 1997



Copyright © 1997 Bay Networks, Inc.

All rights reserved. Printed in the USA. September 1997.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FN, FRE, GAME, LN, Optivity, PPX, Quick2Config, and Bay Networks are registered trademarks and Advanced Remote Node, ANH, ARN, ASN, Bay•SIS, BayStack, BayStream, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, IP AutoLearn, PathMan, RouterMan, SN, SPEX, Switch Node, System 5000, Bay Networks Press, and the Bay Networks logo are trademarks of Bay Networks, Inc.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as “Software” in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price

1. License Grant. Bay Networks, Inc. (“Bay Networks”) grants the end user of the Software (“Licensee”) a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks’ and its licensors’ confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee’s facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee’s intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee’s requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor’s product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of

its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

About This Guide

Before You Begin	xvi
Conventions	xvii
Acronyms	xviii
Ordering Bay Networks Publications	xxii
Bay Networks Customer Service	xxiii
How to Get Help	xxiii

Chapter 1 Introduction

Preventing Problems	1-1
Reading the Release Notes and Relevant Documentation	1-2
Minimizing Disruption When Installing New Software	1-2
Selecting the Proper Tool for Configuring a Router	1-2
Saving Your Configuration Changes	1-3
Backing Up Your Files	1-3
Maintaining Consistent Files in Multiple Flash Memory Cards	1-3
Handling Flash Memory Cards to Prevent Static Damage	1-4
Responding to a Failed prom Command	1-4
Preparing to Troubleshoot	1-4
Getting Acquainted with the Troubleshooting Tools	1-4
Using the System Log to Display Event Messages	1-5
Displaying and Changing Configuration Settings and Statistics	1-10
Using the ping Command	1-20
Using the Packet Capture Tool	1-20
Using Inbound Telnet to Access the Technician Interface	1-21
Taking a Snapshot of Your Network	1-22
Documenting Each Step	1-23
Performing One Corrective Task at a Time	1-24

Chapter 2

Determining the Scope of a Problem

Chapter 3

Troubleshooting an Operational Problem

Damaged Router	3-2
Power Problem	3-2
Blown Fuse	3-2
LEDs Are Off	3-3
Router Won't Boot	3-3
Checking the Boot PROMs	3-6
Making Sure the Router Software Image Is Correct	3-6
Making Sure All Slots Use the Same Router Software Image and Configuration File ...	3-6
Verifying That the Router Software Images in Each Processor Match	3-7
Verifying That the Configuration Files in Each Processor Match	3-9
Lost Password (BN Routers)	3-10
No Space Left on Memory Card	3-11
Memory or Buffer Problem	3-12
Bad Forward Receive Buffer Checksum Errors	3-17
Finding the Slot That Sent a Bad Backplane BofL Packet	3-18
Finding the Slot That Sent a Bad Packet That Was Not a BofL Packet	3-19
Fault Message	3-20

Chapter 4

Troubleshooting a Physical Media Problem

Making Sure the Link Module Is Working	4-1
Determining the Media-Specific State	4-1
Troubleshooting the Cable Connection	4-3

Chapter 5

Troubleshooting a Data Link Layer Problem

Troubleshooting an ATM Connection	5-2
Interface Problems	5-2
Dropped Frames	5-5
ATM VC Mod Failed Message	5-5

Upper-Layer Protocols Failing to Pass Packets	5-6
PVC Problems	5-7
Troubleshooting ATM LANE	5-7
Troubleshooting an Ethernet Connection	5-9
Troubleshooting a FDDI Connection	5-14
Troubleshooting a Frame Relay Connection	5-17
Log Messages from Frame Relay Indicate Circuit Is Down	5-17
Frame Relay Switch Keeps Marking the Circuit as Down	5-18
Frame Relay Circuit Up, but Protocol Data Is Not Transmitting	5-18
PVC Transmitting, but Not Receiving	5-18
Frame Relay Configured with LMI Invokes an Xoff State	5-19
Troubleshooting an MCT1 Connection	5-20
Troubleshooting a Synchronous Connection	5-22
Checking the Address Format (Bay Networks Standard Only)	5-24
Troubleshooting a Synchronous to X.21 Connection	5-24
Reception Errors Incrementing or Reception Count Not Incrementing	5-24
Troubleshooting the Internal Clock Settings (Lab Environments Only)	5-26
Troubleshooting a Token Ring Connection	5-27
Troubleshooting Other Data Link Layer Protocols	5-29

Chapter 6

Troubleshooting a Network Layer Problem

Troubleshooting AppleTalk	6-2
Local Net Range Conflict Event Message	6-3
Zone . . . Conflict Event Message	6-3
Static Configuration Conflict Event Message	6-4
Troubleshooting DLSw	6-4
Troubleshooting IP	6-6
Troubleshooting Telnet, FTP, and TFTP	6-8
Ping Does Not Work	6-9
Router Cannot Ping Another Local Device	6-10
Router Cannot Ping Endstation, Can Ping Other Endstations on the Same Segment	6-11
Endstation Cannot Ping the Remote Interface on the Router	6-11

Endstation Can Ping Devices on the Same Segment, but Cannot Ping the Router	6-12
Endstation Can Ping Local and Remote Interfaces on the Router, but Cannot Ping a Remote Station	6-14
Troubleshooting RIP	6-14
Troubleshooting OSPF	6-15
Troubleshooting IPX	6-16
Troubleshooting OSI	6-21
Troubleshooting Switched Services	6-23
Master Cannot Connect to Slave	6-25
Troubleshooting RS-232 Raise DTR Dial Services	6-25
Troubleshooting V.35 Raise DTR Dial (Balanced)	6-26
Troubleshooting ISDN BRI and PRI	6-27
Troubleshooting Other Network Layer Protocols	6-30

Chapter 7

Troubleshooting a Site Manager Problem

Site Manager Won't Start	7-1
Site Manager Won't Start on a PC	7-1
Cannot Find File Message	7-2
Working Directory or Path Is Invalid Message	7-3
Unable to Find UDP Port Numbers for SNMP Message	7-3
Site Manager Won't Start on a UNIX Workstation	7-3
Unable to Load SNMP MIB or File Was Inaccessible Message	7-4
Unable to Run . . . Module Message	7-4
Cannot Establish a Site Manager Session with the Router	7-5
Using an Alternative Site Manager Workstation to Enable Access	7-5
Using the Technician Interface to Enable Access	7-6
Cannot Connect Site Manager Running on a PC	7-7
Cannot Connect Site Manager Running on a UNIX Workstation	7-8
Target Does Not Respond (or Similar Message)	7-9
Cannot Allocate Colormap Message	7-9
UNIX Workstation Generating Core Dumps	7-9

Chapter 8

Getting Help

Reporting a Problem to the Bay Networks Technical Solutions Center	8-1
Sending and Retrieving Files	8-3

Appendix A

Reading the Event Log

System Startup	A-2
Dial-on-Demand Raise DTR Log	A-18
Dial-on-Demand V.25bis	A-23
MCT1 Log Information in a Lab Environment	A-29

Appendix B

Using the Technician Interface to Configure and Run Packet Capture

Overview	B-2
Implementation Notes	B-4
Getting Started	B-5
Preparing Packet Capture to Run	B-5
Assigning the Processors to Run Packet Capture	B-5
Creating an Instance of Packet Capture	B-7
Allocating Memory for the Packet Capture File	B-11
Specifying the Number of Bytes in Each Packet to Copy	B-12
Enabling Packet Capture	B-12
Starting Packet Capture	B-13
Terminating Packet Capture	B-13
Using the Technician Interface to Display a Packet Capture File	B-14
Deleting a Packet Capture Instance	B-17
Using Optional Features	B-18
Configuring the Direction of the Packets to Be Copied	B-18
Configuring a Termination Trigger	B-19
Assigning Filters	B-21
Setting the Filter Response to a Match	B-22
Specifying the String to Compare with the Packet Data	B-23
Specifying the Data to Compare with the String	B-23
Selecting the Number of Filters That Must Match	B-26
Configuration Examples	B-27
Displaying the Current Packet Capture Configuration Settings	B-30

Displaying Event Messages Issued by Packet Capture	B-31
Using a Sun Workstation or DOS PC to Display Packets	B-31
Getting the Name of the Packet Capture File	B-32
Using FTP to Transfer the File	B-32
Using TFTP to Transfer the File	B-33
Using XMODEM to Transfer the File	B-35
Displaying the File with Packet Dump	B-35
Converting a Packet Capture File to Network General Sniffer Format	B-36
Reference Guide to Packet Capture	B-38
Displaying the Packet Capture Attribute Names and Numbers	B-38
Packet Capture Parameter Descriptions	B-39
Basic Parameters	B-40
Trigger Parameters	B-45
Filter Parameters	B-46
Media-Specific Instructions and Examples	B-51
CSMA/CD	B-51
Protocols Supported by Synchronous, T1, E1, and MCT1 Media	B-52
Token Ring	B-56
FDDI	B-56
HSSI	B-56
ISDN	B-57
Interpreting a Packet Capture Instance Number	B-57

Appendix C

Packet Configuration

Using the Line Subcommand	C-2
Using the Load Subcommand	C-5
Using the Unload Subcommand	C-5

Index

Figures

Figure 1-1.	Filtering Parameters Window	1-6
Figure 3-1.	Verifying the Slot ID on an ASN	3-5
Figure 3-2.	Finding the Slot Receiving Buffer Checksum Errors	3-17
Figure 3-3.	Finding the Slot Number When the Buffer Checksum Message Does Not Reference a Backplane BofL Packet	3-19
Figure 6-1.	Comparing the Endstation and Router Configurations	6-13
Figure 7-1.	Cannot Find File Error Message	7-2

Tables

Table 1-1.	Technician Interface Event Message Filters	1-7
Table 1-2.	Example of an Object Named House	1-12
Table 3-1.	ASN Front-Panel Status Indicators	3-4
Table 3-2.	ASN Rear-Panel SPEX Module Status Indicators	3-4
Table 3-3.	Memory Available for Router Processor Types	3-13
Table 4-1.	State Attribute Values	4-2
Table 5-1.	First Set of ATM Interface MIB Objects to View	5-3
Table 5-2.	ATM Interface Attributes for Troubleshooting	5-3
Table 5-3.	Second Set of ATM Interface MIB Objects to View	5-4
Table 5-4.	Troubleshooting Dropped Frames	5-5
Table 5-5.	Error Codes in the “ATM VC mod failed” Log Message	5-6
Table 5-6.	ATM LANE MIB Objects to View	5-8
Table B-1.	Packet Capture Module Numbers for ARN Interfaces (Except Synchronous)	B-4
Table B-2.	Determining the Slot Mask	B-6
Table B-3.	Structure of a Line Number	B-58

About This Guide

If you are responsible for isolating and solving problems associated with Bay Networks® routers, read this guide.

If you want to	Go to
Prevent problems and prepare to troubleshoot	Chapter 1
Determine the scope of a problem	Chapter 2
Solve problems with the basic operation of hardware and software	Chapter 3
Solve physical media problems	Chapter 4
Solve data link layer problems	Chapter 5
Solve network layer problems	Chapter 6
Solve Site Manager problems	Chapter 7
Report problems to the Bay Networks Technical Solutions Center	Chapter 8
Read and understand the event log	Appendix A
Use the Technician Interface to configure and run Packet Capture	Appendix B
Configure the Packet Capture utility	Appendix C

This guide assumes you have the following background:

- Experience configuring and managing Bay Networks routers
- A working knowledge of Site Manager and the Technician Interface
- A working knowledge of the protocols running on your routers

Before You Begin

Before using this guide to solve a problem, see the following documents:

- *Release Notes for Router Software Version 12.00*
- *Release Notes for Site Manager Software Version 6.00*
- *Known Anomalies: Router Software 12.00 and Site Manager 6.00*

This guide assumes that you also have access to the following Bay Networks manuals, which are on the CD-ROM:

- *Using Technician Interface Software*
- *Using Technician Interface Scripts*
- *Configuring and Managing Routers with Site Manager*
- *Event Messages for Routers*
- The manuals associated with the software you are using

Make sure that you are running the latest version of Bay Networks Site Manager and router software. For instructions, see *Upgrading Routers from Version 7–11.xx to Version 12.00*.

Conventions

angle brackets (< >)	<p>Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.</p> <p>Example: if command syntax is ping <ip_address>, you enter ping 192.32.10.12</p>
bold text	<p>Indicates text that you need to enter, command names, and buttons in menu paths.</p> <p>Example: Enter wfsm &</p> <p>Example: Use the dinfo command.</p> <p>Example: ATM DXI > Interfaces > PVCs identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.</p>
brackets ([])	<p>Indicate optional elements. You can choose none, one, or all of the options.</p>
ellipsis points	<p>Horizontal (. . .) and vertical (:;) ellipsis points indicate omitted information.</p>
<i>italic text</i>	<p>Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.</p>
quotation marks (“ ”)	<p>Indicate the title of a chapter or section within a book.</p>
screen text	<p>Indicates data that appears on the screen.</p> <p>Example: Set Bay Networks Trap Monitor Filters</p>
separator (>)	<p>Separates menu and option names in instructions and internal pin-to-pin wire connections.</p> <p>Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu.</p> <p>Example: Pin 7 > 19 > 20</p>
vertical line ()	<p>Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command.</p> <p>Example: If the command syntax is</p> <p>show at routes nets, you enter either show at routes or show at nets, but not both.</p>

Acronyms

AAL	ATM adaptation layer
ACE	Advanced Communications Engine
ALC	adaptation layer control
AMI	alternate mark inversion
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
AT	AppleTalk
ATM	asynchronous transfer mode
AUI	Attachment Unit Interface
B8ZS	binary 8 zero substitution
BDR	backup designated router
BECN	backward explicit congestion notification
BERT	bit error rate test
BofL	Breath of Life
BootP	Bootstrap Protocol
BootPD	BootP Daemon
BRI	Basic Rate Interface
CCITT	International Telegraph and Telephone Consultative Committee (now ITU-T)
CD	carrier detect
CHAP	Challenge Handshake Authentication Protocol
CID	channel identifier
CRC	cyclic redundancy check
CRN	call request number
CSMA/CD	carrier sense multiple access/collision detection
CSU	channel service unit
CTS	clear to send
DCE	data communications equipment
DLCI	data link connection identifier
DLCMI	Data Link Control Management Interface
DLSw	data link switching
DOS	Disk Operating System

DP	Data Path
DPRAM	dual port RAM
DR	designated router
DS	directory service
DS1E1	multichannel T1/E1 driver service
DSAP	destination service access point
DSL	digital subscriber loop
DSR	data set ready
DSU	digital service unit
DTE	data terminal equipment
DTR	data terminal ready
EIA	Electronic Industries Association
ESF	extended super frame
FDDI	Fiber Distributed Data Interface
FDL	facility data link
FECN	forward explicit congestion notification
FRE	Fast Routing Engine
FRE-2	Fast Routing Engine - 2
FSI	FDDI System Interface
FSM	finite state machine
FTP	File Transfer Protocol
GAME	Gate Access Management Entity
GFWD	GAME forward
GH	gate handle
GRPC	GAME RPC
GUI	graphical user interface
HDLC	high-level data link control
HSSI	high-speed serial interface
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
ILACC	integrated local area communications controller
IP	Internet Protocol
IPX	Internet Packet Exchange

ISAP	internal services access point
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ITU-T	International Telecommunications Union - Telecommunications sector (formerly CCITT)
LAN	local area network
LAPB	Link Access Procedure-Balanced
LB	Learning Bridge
LBO	line build out
LCP	Link Control Protocol
LEC	LAN emulation client
LECS	LAN emulation configuration server
LED	light emitting diode
LLC	logical link control
LSDB	link state database
LSP	link state packet
MAC	media access control
MAU	media access unit
MCT1	multichannel T1
MDI-X	media-dependent interface with crossover
MIB	management information base
MTU	maximum transmission unit
NBMA	nonbroadcast multi-access
NIS	network information services
NVFS	nonvolatile file system
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PC	personal computer (also, program counter)
PCAP	Packet Capture utility
PCR	peak cell rate
PDU	protocol data unit
PPP	Point-to-Point Protocol

PROM	programmable read-only memory
PTP	point-to-point (standard protocol)
PVC	permanent virtual circuit
QENET	Quad Ethernet (link module)
RAM	random access memory
RI	ring indicator
RIF	routing information field
RIP	Routing Information Protocol
RJ	registered jack
RLSD	received line signal detection
ROM	read-only memory
RPC	remote procedure call
RQ	rate queue
RTM	routing table manager
SAP	Service Advertising Protocol
SAR	segmentation and reassembly
SCR	sustainable cell rate
SF	super frame
SMDS	switched multimegabit data service
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SPID	Service Profile Identifier
SPEX	Stack Packet Exchange
SQE	signal quality error
SRM	System Resource Module
STM	server table manager
STP	shielded twisted pair
SWSERV	switched access service
TCP/IP	Transmission Control Protocol/Internet Protocol
TEI	terminal endpoint identifier
Telnet	Telecommunication network
TFTP	Trivial File Transfer Protocol
TFTPD	TFTP Daemon

TPE	twisted pair Ethernet
TTL	time to live
ULI	upper-layer indication
UTP	unshielded twisted pair
VC	virtual circuit
VCI	virtual channel identifier
VCL	virtual channel link
VME	VersaModule-Europe
VPI	virtual path identifier
WAN	wide area network
WCLCK	system clock
WINSOCK.DLL	Windows Socket Dynamic Link Library file
ZIP	Zone Information Protocol

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from Bay Networks Press™ at the following numbers:

- Phone--U.S./Canada: 888-422-9773
- Phone--International: 510-490-4752
- FAX--U.S./Canada and International: 510-498-2609

The Bay Networks Press catalog is available on the World Wide Web at support.baynetworks.com/Library/GenMisc. Bay Networks publications are available on the World Wide Web at support.baynetworks.com/Library/tpubs.

Bay Networks Customer Service

You can purchase a support contract from your Bay Networks distributor or authorized reseller, or directly from Bay Networks Services. For information about, or to purchase a Bay Networks service contract, either call your local Bay Networks field sales office or one of the following numbers:

Region	Telephone number	Fax number
United States and Canada	800-2LANWAN; then enter Express Routing Code (ERC) 290, when prompted, to purchase or renew a service contract 978-916-8880 (direct)	978-916-3514
Europe	33-4-92-96-69-66	33-4-92-96-69-96
Asia/Pacific	61-2-9927-8888	61-2-9927-8899
Latin America	561-988-7661	561-988-7550

Information about customer service is also available on the World Wide Web at *support.baynetworks.com*.

How to Get Help

If you purchased a service contract for your Bay Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Bay Networks service program, call one of the following Bay Networks Technical Solutions Centers:

Technical Solutions Center	Telephone number	Fax number
Billerica, MA	800-2LANWAN	978-916-3514
Santa Clara, CA	800-2LANWAN	408-495-1188
Valbonne, France	33-4-92-96-69-68	33-4-92-96-69-98
Sydney, Australia	61-2-9927-8800	61-2-9927-8811
Tokyo, Japan	81-3-5402-0180	81-3-5402-0173

Chapter 1

Introduction

This chapter describes how to prevent router problems and prepare to troubleshoot.

Topic	Page
Preventing Problems	1-1
Preparing to Troubleshoot	1-4
Documenting Each Step	1-23
Performing One Corrective Task at a Time	1-24

Preventing Problems

The following sections offer tips on how to prevent the most common errors that occur:

- [“Reading the Release Notes and Relevant Documentation”](#)
- [“Minimizing Disruption When Installing New Software”](#)
- [“Selecting the Proper Tool for Configuring a Router”](#)
- [“Saving Your Configuration Changes”](#)
- [“Backing Up Your Files”](#)
- [“Maintaining Consistent Files in Multiple Flash Memory Cards”](#)
- [“Handling Flash Memory Cards to Prevent Static Damage”](#)
- [“Responding to a Failed prom Command”](#)

Reading the Release Notes and Relevant Documentation

The release notes and the manuals that describe how to configure and manage the protocols on your network provide guidelines on how to prevent problems. Read them before installing or upgrading router or Site Manager software.

Minimizing Disruption When Installing New Software

When installing or upgrading software, or using a new feature for the first time, test it at a time or on a node that minimizes disruption to the network. Make software changes one node at a time in the network. Doing so will help you to isolate and solve any problems that may occur as a result of the change.

Selecting the Proper Tool for Configuring a Router

Bay Networks recommends that you use the configuration tools as follows:

- Use the Configuration Manager in remote or local mode when you create a new configuration file or make major changes to an existing configuration file.
- Use the Configuration Manager in dynamic mode only to perform minor changes such as changing a filter or adding a port.
- Use the Technician Interface to issue **set** and **commit** commands to make minor configuration changes only if Site Manager is unavailable; the Technician Interface does not perform any error checking.



Caution: Dynamic changes to the router's base records and global parameters can cause an interruption in service. For example, if you change the size of the bridge forwarding table, the router deletes the table and re-creates it, causing a temporary decline in performance. Therefore, you may want to schedule such changes to minimize the impact on your network.

Saving Your Configuration Changes

The router overwrites the configuration changes in memory when it reboots. If you use either the Configuration Manager in dynamic mode or the Technician Interface **set** and **commit** commands to change the file in memory, you must perform the following procedures if you want to save your changes:

- If you use the Configuration Manager in dynamic mode to make changes, choose File > Save or File > Save As to copy the configuration from memory to the media; otherwise, the changes will be lost when the router reboots.
- If you use the Technician Interface **set** and **commit** commands, you must enter the following command to copy the modified configuration from memory to the media:

save config <volume>:<filename>

Backing Up Your Files

Store backup copies of the configuration files on the Site Manager workstation. To prevent confusion, use a log to record the location, name, and purpose of each configuration file you back up. Organizing and naming the backup files on the Site Manager workstation will also help to prevent mix-ups.



Caution: Always back up a file before deleting it. This includes configuration and log files. In addition, always back up the current log file on the Site Manager workstation before clearing it; you may want to refer to it later to troubleshoot a problem.

Maintaining Consistent Files in Multiple Flash Memory Cards

If the router uses multiple flash memory cards, make sure that each file is consistent on each flash memory card designated for storing files of that type. For example, if you make a change to a router software image or configuration file, save the file to each flash memory card that contains the same files.

To make sure that the files of the same name are consistent on multiple flash memory cards, display each card's directory contents and compare the size of each file.

Handling Flash Memory Cards to Prevent Static Damage

Always use an antistatic wrist strap when handling flash memory cards; static electricity can damage them.

Responding to a Failed prom Command



Caution: If the Technician Interface **prom** command fails, do not reboot. Instead, call the Bay Networks Technical Solutions Center.

If you reboot after the **prom** command fails, a Bay Networks representative must insert new PROM (programmable read-only memory) components on the router baseboard and write new PROM software to them before the router can recover.

Preparing to Troubleshoot

The following sections describe how to prepare to troubleshoot router problems:

- “Getting Acquainted with the Troubleshooting Tools”
- “[Taking a Snapshot of Your Network](#)”

Getting Acquainted with the Troubleshooting Tools

Troubleshooting is much more complicated when you have to solve a problem that requires an urgent solution, and at the same time learn how to use the tools to solve the problem. Read this section and familiarize yourself with the tools before you begin troubleshooting. The instructions later in this guide assume you can use the tools described in this section.

Read the following sections:

- “[Using the System Log to Display Event Messages](#)”
- “[Displaying and Changing Configuration Settings and Statistics](#)”
- “[Using the ping Command](#)”
- “[Using the Packet Capture Tool](#)”
- “[Using Inbound Telnet to Access the Technician Interface](#)”

Using the System Log to Display Event Messages

The processor that is running software in each slot maintains its own log file in local memory. Software entities (such as CSMA/CD and IP) report messages when routine and noteworthy events occur. When you instruct Site Manager or the Technician Interface to display the messages, the router automatically assembles the messages from all slots into a single file and displays the file. Use the messages in this file to diagnose a problem with a port, slot, router, or protocol.

You can use the Technician Interface **log** command to display the log in the router's memory, or use the Events Manager tool's File > Get Current File option to display it. See *Event Messages for Routers* for descriptions of the format and meaning of the event messages.



Note: When using the Events Manager tool to display a log, choose the Descending Order option. If you do this, the Events Manager displays the most recent event messages first. If you display a log in ascending order, and the log contains more events than the maximum that the Events Manager can open, it may not be able to display the most recent events.

When you view a log or save it to a flash memory card, the router combines log files from each processor into a single file and sorts the events by date and time.

If a fault event message appears in the log, use the procedures in this guide to help you isolate and correct the problem. If you cannot recover from the fault, contact the Bay Networks Technical Solutions Center for the appropriate action to take.



Caution: Always save a copy of the entire log to your flash memory card when a fault appears. The router saves the log to a flash memory card only when you issue the Technician Interface **save log <filename>** command. The format of the log file is binary. If you request help from the Bay Networks Technical Solutions Center, you may need to provide the binary version of the log file to troubleshoot the problem. Do not delete the log file from the router until you are sure you have solved the problem.

After viewing all event messages that pertain to a specific problem, and before running tests to isolate the problem, you may want to issue the Technician Interface **clearlog** command or choose Events Manager Administration > Clear log to remove all previously logged events from the event log. Bay Networks recommends that you save the log before you clear it.

If you want to save a log in ASCII format, choose File > Save Output to Disk from the Events Manager window.

A processor keeps its log file even if you reset its router slot. The processor will lose the event messages generated in the slot only if one of the following occurs:

- You clear the log.
- The router software diagnostic tests run.
- The processor board loses power because you removed it, a fuse blew, or the router lost power.

Filtering Event Messages

You can use the Technician Interface or Events Manager to filter the display of event messages. In the Events Manager Configuration Filters window, choose View > Filters to display the Filtering Parameters window (Figure 1-1).

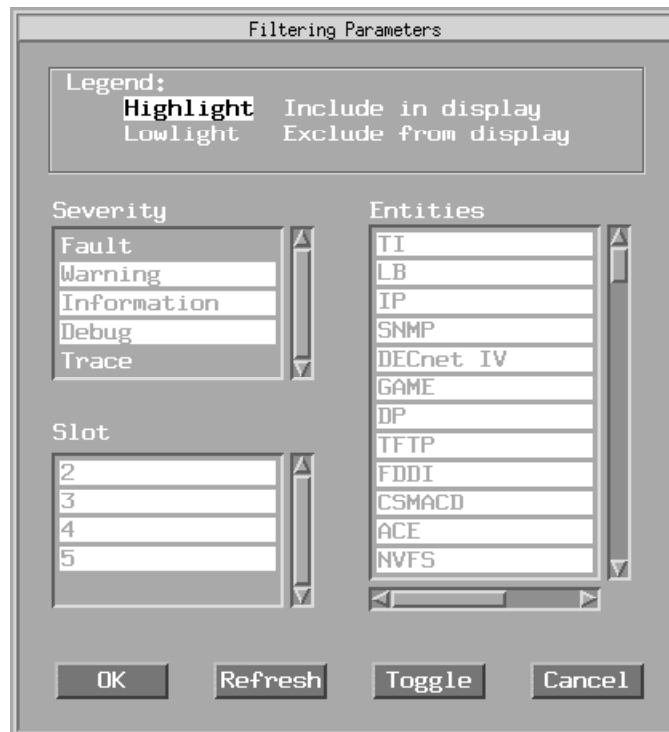


Figure 1-1. Filtering Parameters Window

The Filtering Parameters window allows you to filter based on the severity of the event messages, the software entity reporting them, and the number of the slot from which the entity reported them.

The Technician Interface **log** command supports optional arguments you can use to filter the display of event messages (Table 1-1).

Table 1-1. Technician Interface Event Message Filters

To Filter Events By	Use the Following Technician Interface Command Syntax	Technician Interface Command Example
The software entity (such as IP) that reported the events Note: Always use upper-case letters when specifying a software entity.	log -e <entity>	log -eIP
The slot number of the processor that reported the events	log -s <slot_no.>	log -s3
The severity of the events. The severity types are fault, warning, trace, informational, and debug. When using the Technician Interface to filter events, use the first letter of the severity type.	log -f <f w t i d>	log -ff
Starting date and time (Technician Interface only)	log -d <mm/dd/yy> -t <hh:mm>	log -d10/29/97 -t11:00

See *Event Messages for Routers* for a description of each severity type.



Note: If you use Site Manager or the Technician Interface to display the log without filtering explicitly by the severity type, the log displays only fault, warning, and informational events.

If you are using the Events Manager to view a log and you change the filters, you must refresh (or redisplay) the event log to use the new filters.

You can specify filters for more than one severity type. The Events Manager's Filter window allows you to select more than one filtering option, and the Technician Interface allows you to specify more than one filter. The following command displays all of the events:

log -ffwtid

You can use the Technician Interface or Events Manager to combine the filters. For example, you enter the following command to display all IP events from 11:19 on 10/29/97:

log -eIP -d10/29/97 -t11:19 -ffwtid

You can filter more than one software entity, slot number, and severity type, and combine filter types. The following command filters all severity types from Ethernet and IP running on slots 3 and 4.

log -ffwtid -eCSMACD -eIP -s3 -s4

See the following guides for detailed information about using the event log:

- *Configuring and Managing Routers with Site Manager*
- *Using Technician Interface Software*
- *Event Messages for Routers*

Understanding Debug Messages in the Event Log

The debug severity type often raises many questions. Debug messages help Bay Networks engineers troubleshoot problems. Many debug messages refer to lines of code and memory addresses that are meaningless to you. For this reason, *Event Messages for Routers* does not describe the debug messages.



Note: Do not become alarmed at debug messages. They appear routinely in the log. Use the fault, warning, informational, and trace message severities as your primary filters for debugging problems before looking at the debug messages. By default, Site Manager and the Technician Interface do not display debug messages unless you use the debug filter.

However, displaying the debug messages can help you to understand the systematic process the software uses to load and initialize discrete software components. When the software detects a problem, the debug messages can show you the systematic process the software uses to isolate its components, shut them down, and restart them to try to fix the problem.

Many debug messages are meaningless in isolation, but when considered in the context of other messages, they can help you to understand the problem. Debug messages typically contain words such as “creating,” “dying,” “killing,” “gates,” and “gate handles.”

The name of the router’s operating system is GAME (Gate Access Management Entity). In addition to assuming the typical responsibilities of an operating system, GAME creates gates.

Each gate is a process. The process may perform a discrete action for a software entity, such as IP; or, it may create child gates responsible for their own processes. A parent gate keeps track of its child gate by remembering its logical address, called a gate handle.

If you configure the router to run IP, the gate responsible for creating protocols creates an IP gate. This gate in turn creates gates for IP processes, such as RIP or OSPF. RIP and OSPF gates create gates of their own to handle RIP and OSPF processes. Thus, each time the operating system starts, it creates gates that form a hierarchy resembling a family tree.

If the software detects a problem, it instructs the parent gate to “kill” (eliminate from memory) the gate associated with the problem, and then re-create it. If the problem recurs, the software instructs the grandparent gate to kill its children and re-create them. When a gate “dies” (is eliminated), all of its children also die. The grandparent re-creates the parent gate, and the parent gate re-creates its children. This process expands to the next generation and continues until the problem is resolved or the software entity reinitializes. GAME generates a fault event message when it reinitializes a software entity. This system of creating and killing gates allows the software to try to correct a problem, but minimizes the impact to the network because it resets only the components that are associated with the problem.

See Appendix A for examples and explanations of debug messages.

Displaying and Changing Configuration Settings and Statistics

The router's management information base (MIB) determines its configuration and state of operation. The following sections describe how to access the MIB variables:

- [“Using the Technician Interface to Access the MIB”](#)
- [“Using the Technician Interface Scripts to Access the MIB”](#)
- [“Using the Statistics Manager to Access the MIB”](#)

Using the Technician Interface to Access the MIB

The Technician Interface is an out-of-band router management and troubleshooting tool. When the Site Manager connection to the router is unavailable, you can use the Technician Interface as a remote management tool to manage the router and troubleshoot the problem. *Using Technician Interface Software* explains how to connect a modem to the router to establish a remote Technician Interface session.

The internal structure of the MIB contains the following:

- **Objects.** An object is a collection of MIB objects that store data to serve a special purpose.
- **Attributes.** An attribute is a variable (parameter).
- **Instances.** An instance is a physical manifestation of an attribute.
- **Values.** A value is the data stored in a location indexed by an object, an attribute associated with that object, and an instance of that attribute.

Suppose you are shopping for a house and a car, and you want to create databases of information about houses and cars on a computer. You create tables (*objects*) named House and Car to store this information.

You assign each object a unique number (*object identifier*). For example, the object identifier for House is 1 and Car is 2. You can access information about houses by naming the object (House) or by using its object identifier (1).

You create *attributes* to describe each object. For example, you create house attributes such as list price, size of lot, color, town, street, house number, garage or no garage, number of bedrooms, total square feet, and how much you like it on a scale of 1 to 10.

You assign each attribute a unique number called an *attribute identifier*. For example, you use 1 for list price, 2 for size of lot, 3 for color, etc.

To access the size of lot, you can specify the object by name (House) or by identifier (1), and the attribute by name (SizeOfLot) or by number (2) in the format House.SizeOfLot or 1.2.

Now you can list the attributes of House by name and number using the command **list House**.

Example

list House

```
ListPrice = 1
SizeOfLot = 2
Color = 3
Town = 4
Street = 5
House = 6
Garage = 7
Bedrooms = 8
TotalSquareFeet = 9
HowMuchILikeIt = 10
```

Whenever the number of values of an object is limited, you assign code numbers to the values. For example, for the Color attribute of the object House, you use 1 for white, 2 for green, 3 for brown, etc.

Until now, we've been discussing houses in abstractions, not physical manifestations. To reference particular houses, you select attributes that, by themselves, uniquely identify the houses. For example, several houses have a 10,000 square foot lot, but a particular house you have seen is blue. The attribute Color.TotalSquareFeet identifies the house.

An *instance* is the MIB name for a collection of attribute values that uniquely identify particular objects. If more than one blue house has a 10,000 square foot lot, you need the attributes town, street, and house number (House.Street.Town) to uniquely identify the house. The instance value 221.Main.Middleton identifies the house at 221 Main Street in the town of Middleton.



Note: Do not confuse object or attribute identifiers with values. Identifiers are numbers you can use in place of attribute names.

Table 1-2 presents the attributes and instances for the example object House. The attributes and instances are in bold, and the instance values are in regular print.

Table 1-2. Example of an Object Named House

Attributes and Identifiers	Instances		
	221.Middleton	10.Easton	42.Weston
ListPrice (1) in thousands of dollars	150	160	170
SizeOfLot (2) in thousands of square feet	10	20	10
Color (3) (1 = white, 2 = green, 3 = brown)	2	1	1
Town (4)	Middleton	Easton	Weston
Street (5)	Main	Pleasant	Elm
HouseNo (6)	221	10	42
Garage (7) (0 = none, 1 = one-car, 2 = two-car)	0	1	1
Bedrooms (8)	3	3	2
TotalSquareFeet (9) in thousands of feet	15	18	12
HowMuchILikelt (10) (1 - 10; 10 is the highest rating)	7	6	3

If you created this hierarchy of the object House, you could specify an instance of House using an identifier for each object, from the top of the hierarchy to the instance.

For example, to display the color code of the house at 10 Pleasant Street in Easton, you could enter one of the following commands:

- **get House.Color.10.Pleasant.Easton**
- **get 1.3.10.Pleasant.Easton**

In this example, you specify the object identifiers in place of House.Color.

Suppose you create several diverse objects and you want to organize them. You can create an object to organize and provide access to objects that fit into the same category.

For example, you could create an object named `ItemsToPurchase` to store the objects `House` and `Car`. You could then further group the `ItemsToPurchase` with an object named `Inventory` by putting them both in an object named `Things`.

The router software uses a large hierarchy of objects that together form the MIB. The software uses the data in these objects to configure itself and to determine its behavior in the network, just as you would have used the data to select a house.

You can view all the object names in the router's MIB by entering the Technician Interface **list** command. The following example shows a small portion of the list of objects you can display with this command. The numbers to the right of the equals sign (=) are not values; they are the numeric identifiers of these objects, which you can use in place of the object name. When using the Technician Interface, it is easier to use the object names.

Example

```
list
wfCSMACDEntry = 1.3.6.1.4.1.18.3.4.1.1
wfCSMACDAutoNegEntry = 1.3.6.1.4.1.18.3.4.16.1.1
wfFddiEntry = 1.3.6.1.4.1.18.3.4.4.1
```

A dot (.) separates each object. The objects in the example belong to a hierarchy of objects identified by 1.3.6.1.4.1.18.3.4.

You can view all the attribute names and numeric identifiers of an object by entering the Technician Interface **list <object>** command.

Example

```
list wfCSMACDEntry
wfCSMACDDelete = 1
wfCSMACDEnable = 2
wfCSMACDState = 3
wfCSMACDSlot = 4
wfCSMACDConnector = 5
wfCSMACDCct = 6
wfCSMACDBofl = 7
wfCSMACDBoflTmo = 8
wfCSMACDMtu = 9
wfCSMACDMadr = 10
```

For example, the object identifier of wfCSMACDMadr (the media access control address) is 10. When entering the object and attribute in Technician Interface commands to display or change a value, you specify the object by name (wfCSMACDMadr) or by number (1.3.6.1.4.1.18.3.4.1.1), and you specify the attribute by name (wfCSMACDMadr) or by number (10). Thus, you can specify the combined object and attribute (object.attribute) in one of the following ways. (The first way is the best because you are less likely to make a typing error.)

- wfCSMACDEntry.10
- wfCSMACDEntry.wfCSMACDMadr
- 1.3.6.1.4.1.18.3.4.1.1.wfCSMACDMadr
- 1.3.6.1.4.1.18.3.4.1.1.10



Note: The files that describe the MIB are in the */mibs* subdirectory. The default UNIX directory path to the MIB files is */usr/wf/mibs*. The default DOS directory path to the MIB files is *\wf\mibs*. The files identify and describe each MIB attribute. If the valid values of an attribute are finite, the associated MIB lists them. Use a text editor to perform searches of objects that interest you.

You can view all the instances of an object configured on the router by entering the Technician Interface **list instances** *<object>* command.



Note: Objects, such as wfIpxBase and wfIpBase, that include scalar objects always have the single instance identifier 0.

Example

```
list instances wfCSMACDEntry
    inst_ids  = 1.1
               1.2
               10.1
               10.2
```

The instance format of the wfCSMACDEntry object is slot.connector. In this example, connectors 1 and 2 in slots 1 and 10 are the instances of the wfCSMACDEntry object.

To determine the format of an instance, search for the name of the object in the associated MIB file (*<object>.mib*) until the specification of the object appears. The INDEX field describes the format of the instance associated with that object.

Example

This example shows that the slot and connector form the instance of all attributes of the object named wfCSMACDEntry:

```
wfCSMACDEntry OBJECT-TYPE
    SYNTAX wfCSMACDEntry
    ACCESS not-accessible
    STATUS mandatory
    DESCRIPTION
        " An entry in the csmacd table "
    INDEX      { wfCSMACDSlot,
                 wfCSMACDConnector }
    ::= { wfCSMACDTable 1 }
```

Use a dot (.) instead of a comma to separate the elements of an instance. Thus, you express slot 10, connector 1 as 10.1 when using the Technician Interface to get or change the values of attributes associated with this instance.

Example

This example shows the instances of the object wfIpInterfaceEntry. The instance format differs from that of the object wfCSMACDEntry.

```
list instances wfIpInterfaceEntry
inst_ids = 1.1.1.1.100
           1.1.2.1.101
           1.1.3.1.102
           1.1.4.1.103
           1.2.1.1.2
```

The INDEX field in the specification of the object wfIpInterfaceEntry in the *ip.mib* file shows that the instance format consists of the address of the IP interface and the circuit number:

```
wfIpInterfaceEntry OBJECT-TYPE
    SYNTAX wfIpInterfaceEntry
    ACCESS not-accessible
    STATUS mandatory
    DESCRIPTION
        " An IP interface description "
    INDEX      { wfIpInterfaceAddr,
                 wfIpInterfaceCircuit }
    ::= { wfIpInterfaceTable 1 }
```

You can use the following Technician Interface commands to access the MIB:



Caution: The Technician Interface does not perform any error checking when you change the value of a MIB attribute. Whenever possible, use Site Manager to change configuration settings. If you do use the Technician Interface, refer to the appropriate MIB file to determine which values are valid. Invalid values can disrupt the operation of the router.

- **list** displays the object names and their associated numeric identifiers, as described earlier.
- **get** *<object>.<attribute>.<instance>* displays the value of an object.
- **set** *<object>.<attribute>.<instance>* *<value>* changes the value of an object.

You enter **set** commands to make changes to configuration settings. Note the space between *<instance>* and *<value>*.

- **commit** changes the value in volatile memory.

Enter the **commit** command after issuing **set** commands, or the **set** commands will not work. (When you use the Configuration Manager to make changes and choose File > Save, the router automatically changes the value in volatile memory.)



Caution: When you change the setting of a base protocol object, the modified protocol may restart. Consequently, network users may lose their connections. If possible, schedule such configuration changes at a time that will minimize network disruption.

Remember to save the changes to a file on the router's flash memory card or floppy disk before rebooting. You can do this using the Configuration Manager or the Technician Interface. When using the Configuration Manager in dynamic mode, choose File > Save. When using the Technician Interface, enter the following command:

save config *<volume>:<filename>*

If you do not specify *<volume>*, the router saves the file to the default volume.

Object and attribute names can be long and are case-sensitive. To reduce errors, Bay Networks recommends that you use the number of an attribute rather than name it.

When entering a **get** command, you can use an asterisk (*) in place of an attribute to display all of the attribute values of an instance. For example, the following command displays the value of each attribute of the instance 10.1 (slot 10, connector 1).

```
$ get wfCSMACDEntry.*.10.1
wfCSMACDEntry.wfCSMACDDelete.10.1 = 1
wfCSMACDEntry.wfCSMACDEnable.10.1 = 1
wfCSMACDEntry.wfCSMACDState.10.1 = 1
wfCSMACDEntry.wfCSMACDSlot.10.1 = 10
wfCSMACDEntry.wfCSMACDConnector.10.1 = 1
wfCSMACDEntry.wfCSMACDCct.10.1 = 19
```

You can also use an asterisk in place of the instance in a **get** command to display all of the values of a single attribute. For example, the following command displays the wfCSMACDState of all of the instances. The specification of the wfCSMACDState attribute in the *csmacd.mib* file states that 1 means up and 2 means down. Note that you can use this method to display all instances without having to enter the **list instances <object>** command.

```
get wfCSMACDEntry.3.*
wfCSMACDEntry.wfCSMACDState.1.1 = 1
wfCSMACDEntry.wfCSMACDState.1.2 = 2
wfCSMACDEntry.wfCSMACDState.10.1 = 1
wfCSMACDEntry.wfCSMACDState.10.2 = 1
```



Note: You can use an asterisk in place of the attribute or instance in a **get** command, but you cannot use an asterisk in place of both.

You can use the complete MIB number in place of the *<object>.<attribute>* specification. The parameter descriptions in the configuration manuals list the MIB number for this reason. SNMP commands also use this syntax.

If you enter a **get** command and the message object does not exist appears, do the following:

1. **Check the spelling and case of the object name.**
2. **Configure and enable the object.**

See *Using Technician Interface Software* for detailed instructions on how to use the Technician Interface to display and change the values in the MIB.

The advantage of using the Technician Interface scripts, the Statistics Manager, or the Configuration Manager instead of the Technician Interface commands is that you don't have to know an object, attribute, and instance in order to display or change a setting. The next two sections introduce you to the Technician Interface scripts and the Statistics Manager. This guide assumes that you already know how to use the Configuration Manager.

Using the Technician Interface Scripts to Access the MIB

Technician Interface script files are simple programs consisting of one or more SNMP **get** commands that allow you to display menus and values of MIB objects without having to understand the MIB.

To enter script commands, do the following:

1. **Use FTP or TFTP to transfer the script files to a flash memory card installed in the router.**
2. **Enter the run `setpath` command to access the `setpath.bat` file to tell the router where to look for the script files.**

You can then enter the **show** or **monitor** script command, specifying the name of the script menu you want to display. The **show** command displays the statistics at the time you request them. The **monitor** command displays statistics at the time you request them, and continues to refresh the display so that you can see any changes to them.

As you become more proficient with the scripts, you can specify a script menu option without having to display a menu. For example, the **show at** command displays the AppleTalk script menu, which includes the AARP table option. The **show at aarp** command displays the AARP table.

See *Using Technician Interface Scripts* for detailed instructions on setting up, loading, and using the scripts.

Using the Statistics Manager to Access the MIB

The Statistics Manager tools allow you to monitor a router's status and performance from the Site Manager workstation. You can access the statistical values in the MIB by using the following options in the Tools menu of the Statistics Manager window:

- The **Quick Get** tool allows you to click your way down the MIB tree to a MIB attribute and retrieve its values. Because the Quick Get tool is fast and does not require an initial setup of the screens, this guide refers to it as an alternative to using the Technician Interface or the scripts.

The Quick Get tool features a Description button and a Retrieve button.

If you click on an attribute and click on Description, a new window displays the description of the attribute from the MIB specification.

If you click on an attribute and click on Retrieve, Site Manager retrieves and displays all of the values of that attribute. You can retrieve more than one attribute at a time.

- The **Screen Manager** tool allows you to select windows of statistics from the Default Screens window, which contains a list of statistics windows provided with Site Manager. You can then do the following:

- Add these windows to the Current Screens List window so that you can launch them.
- Copy these windows to the User Screens window so that you can customize them.

- The **Launch Facility** tool allows you to select and display a statistics window from the list of statistics windows you added to the Current Screens List window.

When you launch a statistics window, the Statistics Manager queries the router for the values and displays them.

- The **Screen Builder** tool allows you to do the following:
 - Build windows of statistics from scratch.
 - Customize statistics windows you copied to the User Screens window.

See *Configuring and Managing Routers with Site Manager* for detailed instructions on using the Statistics Manager.

Using the ping Command

The **ping** command is available both from the Site Manager Administration menu and the Technician Interface. When you enter the **ping** command, the router, not Site Manager, issues an Internet Control Message Protocol (ICMP) echo request. Options include packet size, number of repetitions, and the ability to trace the path of the ICMP echo request.

When you lose AppleTalk, APPN, IP, IPX, OSI, or VINES connectivity, use the **ping** command to isolate the problem interface. Try pinging the end node that has connectivity problems. If you fail to get a response, ping the local router interface, and then ping each router interface along the way to the problem node.

If, after attempting to ping a device, the response is `Unknown Network Or Network Unreachable`, check the local node's routing table and its default gateway definition.

If the **ping** command yields the response `Target does not respond`, the station from which you issued **ping** sent an echo request to the address it has for the end node, but never received a reply. In this case, start pinging each node in the path between the source and destination until you find the problem interface.

See *Using Technician Interface Software* or *Configuring and Managing Routers with Site Manager* for detailed instructions on issuing the **ping** command.

Using the Packet Capture Tool

The Technician Interface Packet Capture tool allows you to filter, send, capture, and view packets in hexadecimal format. You can save the data in a Network General Sniffer format file, transfer the file to a network analyzer, and use the analyzer to parse the data. Bay Networks recommends that you use Packet Capture to capture data generated at remote routers, save it in Network General Sniffer format files, and use TFTP or FTP to transfer the files to a site where you can open them using a network analyzer.

Appendix B provides detailed instructions on how to use Packet Capture.

Using Inbound Telnet to Access the Technician Interface

Versions 7.60 and later allow you to use Telnet to establish a Technician Interface session with a router.



Note: Bay Networks strongly recommends that you learn how to establish an inbound Telnet session with the router in order to troubleshoot problems from a remote site.

To make Telnet a configurable option in the Protocols menu, create and enable TCP and the Telnet server from the Configuration Manager window as follows:

1. **Choose Protocols > Global Protocols > TCP > Create TCP.**
2. **Choose Protocols > Global Protocols > Telnet Server > Create Telnet Server.**

The Telnet Configuration window opens.

3. **Change the settings, or use the default settings, then click on OK.**

Unlike the Series 5 software, more than one user can establish an inbound or outbound Telnet session with a router at the same time. However, Bay Networks does not recommend multiple Telnet sessions because the memory required to maintain multiple TCP connections can affect system performance.

For detailed instructions on how to establish a Telnet connection to a router, see *Using Technician Interface Software*.

To resolve problems, see “Troubleshooting Telnet, FTP, and TFTP” in Chapter 6.

Taking a Snapshot of Your Network

Bay Networks recommends that you periodically gather and save the forwarding and routing tables maintained by the protocols running on each router. You can use the Technician Interface or the Statistics Manager to do this.

Access to this information will be helpful when you are troubleshooting problems in the future. For example, when troubleshooting a problem, you may find the next-hop address to a given destination does not match that in a table you saved previously. This would help you to conclude that there may be a problem with the connection to the node that should be the next-hop address.

You can use the Technician Interface to save tables (or any other Technician Interface displays) to a single file as follows:

1. **Log in as Manager.**
2. **Enter the following command:**
record open <volume>:<filename>
<volume> is the number or letter of the router's file-storage medium.
<filename> is the name of the file you are creating to store the display text.
3. **Display the routing tables.**
4. **Enter the following command to copy the file from memory to the router's file-storage medium and terminate the recording:**
record close
 To learn more about the Technician Interface recording feature, enter this command:
help record

You can use the Statistics Manager to save tables to files as follows:

1. **Use the Statistics Manager Screen Manager tool to add the routing tables in the Default Screens window to the Current Screens List window.**
2. **For each routing table:**
 - a. **Use the Launch Facility tool to display the table.**
 - b. **Use the File > Save option to save the contents of the table to a formatted ASCII file.**

You can use any text editor to read the ASCII files, or print and organize them for later reference.

A map of your network configuration is another useful resource for troubleshooting. Include in the map information about the hardware, software, and cables you are using. When troubleshooting a problem, compare the next hop on the network map to that of the forwarding table associated with the problem protocol.

Documenting Each Step

An effective troubleshooting strategy is to take detailed notes as you perform each procedure. These notes are useful for the following reasons:

- They give you an opportunity to pause and think clearly about the problem and the procedures you are following.

You are more likely to develop a methodical and reasoned approach, and think of solutions during this reflective period.

- They provide you with a record of the tasks you performed. This record is essential for these reasons:
 - You can refer to it during the procedure to recall whether you already performed a certain task.

A diagnostic procedure can include many tasks. It is easy to forget, for example, which statistics you checked and what they revealed at a given time.
 - You can refer to it to determine whether, after implementing a test solution, you repeated important diagnostic steps.
 - You can refer to notes about previous occurrences of the same problem to find hints on how to recover quickly.
 - You can provide the information needed by another interested colleague, manager, or Bay Networks Technical Solutions Center representative if you cannot resolve the problem yourself.

Performing One Corrective Task at a Time

Always perform one corrective task at a time. Then, repeat the test that you performed to identify the problem in order to validate the correction. Verify that the task solved the problem before performing the next corrective task.

This way, you know which task solved the problem. If you perform multiple corrective tasks without verifying the success of each one, you may unknowingly make one of the following mistakes:

- Complicate the original problem
- Solve the problem but cause another
- Solve the problem without knowing how you solved it

Chapter 2

Determining the Scope of a Problem

This chapter poses the initial questions you should answer to narrow the cause of a problem to such topics as router operation, router software, the physical layer, the data link layer, or the network layer. Subsequent chapters provide instructions on how to further isolate and solve problems in each category. The instructions in this chapter tell you which chapters to go to after determining the scope of a problem.

Determine the scope of a problem by researching and writing down the answers to the following questions:

1. What are the symptoms of the problem?

The more information you have about the symptoms of the problem, the more easily you can identify the cause.



Note: The symptoms of a problem and the underlying cause of the problem are not necessarily the same. For example, if you cannot ping an IP router, the symptom is that you cannot ping the router; the cause may be a loose cable.

2. When did each symptom begin?

Write down the time you learned about each symptom. Examine the event log for event messages that indicate when the problem occurred. Read the event message descriptions for clues.

3. What recent changes could have contributed to the problem?

- Reconfiguration?
- Moved nodes?
- Added segments?
- Increased traffic?

4. Are you using a workaround to prevent the symptoms from occurring? If so, what?

Consideration of the workaround you are using may help you to isolate the problem.

5. Which end stations are involved?

Identifying the end stations involved can help you to determine the scope of the problem.

6. Research and consider the following additional causes:

- Traffic congestion

Examine the MIB statistics and the event log to check for traffic congestion. If you determine that traffic congestion is the problem, consider redistributing traffic to relieve congestion.

- A software anomaly

Check the following documents for solutions to your problem:

-- *Release Notes for Router Software Version 12.00*

-- *Release Notes for Site Manager Software Version 6.00*

7. Look at the LEDs on the router's front and rear panels, and refer to the event log and MIB statistics to answer the following questions:

Are the symptoms limited to:

- A single protocol on a single port?

If so, the problem is most likely in the network layer or above. See Chapter 6.

- Multiple protocols on a single port?

If so, the problem is most likely in the physical or data link layer. See Chapters 4 and 5.

- A single protocol on multiple ports in one slot?

If so, the problem is most likely in the configuration of the network layer protocol. See Chapter 6.

- Multiple protocols on multiple ports in one slot?

If so, and if the same protocols are running successfully in other slots, the problem is most likely physical. See Chapter 4.

- A single protocol on multiple ports in all slots running that protocol?

If so, the problem is most likely in the configuration of the network layer protocol. Make sure you enabled the protocol and see Chapter 6.

- Multiple protocols on multiple ports in all slots in the router (box)?

If so, the problem is most likely operational. See Chapter 3.

- Multiple routers?

If so, the problem is most likely due to an external device. Try to determine the cause of the problem.

Chapter 3

Troubleshooting an Operational Problem

This chapter describes how to solve problems with the basic operation of the hardware and software. It assumes that you have already determined the scope of your problem, as described in Chapter 2.

Topic	Page
Damaged Router	3-2
Power Problem	3-2
Blown Fuse	3-2
LEDs Are Off	3-3
Router Won't Boot	3-3
Checking the Boot PROMs	3-6
Making Sure the Router Software Image Is Correct	3-6
Making Sure All Slots Use the Same Router Software Image and Configuration File	3-6
Lost Password (BN Routers)	3-10
No Space Left on Memory Card	3-11
Memory or Buffer Problem	3-12
Bad Forward Receive Buffer Checksum Errors	3-17
Fault Message	3-20

Damaged Router

If you detect physical damage to the router, report the problem to the Bay Networks Technical Solutions Center.

Power Problem

Troubleshoot a power problem as follows:

1. **Make sure the power cable is firmly connected to the router and the electrical outlet.**
2. **Make sure that the Ethernet transceivers have power.**
If they do not, call the Bay Networks Technical Solutions Center.
3. **If the router is a BCN® or CN®, determine whether the circuit breaker broke the power circuit.**
4. **If the router is a BCN or BLN®, check the power supply LEDs.**

If a single power supply LED is off and the power supplies are modular, make sure that all power supply cables are firmly connected. Otherwise, replace the power supply.

If more than one power supply LED is off, remove one power supply. If all of the remaining power supply LEDs light, replace the power supply you removed. Otherwise, reinsert the power supply and remove another. Repeat this procedure until you find the problem power supply.

Blown Fuse

The following events may cause a fuse to blow:

- A power surge.
- You hot-swapped a link module that does not meet the minimum version requirements for hot-swap support.

To determine whether the link module meets hot-swap requirements:

1. **Use your web browser to open the following document:**
<http://support.baynetworks.com/Library/GenMisc/>
2. **Click on Compatibility Matrix - Router.**

To determine whether a fuse has blown in a BLN or BCN, and to isolate and replace a blown fuse, see the *BLN and BCN Fuse Service Manual*.

LEDs Are Off

The LEDs on a Fast Routing Engine (FRE®), System Resource Module (SRM), or link or net module may fail to light for the following reasons:

- The Ethernet transceivers on a slot have lost power.
- A slot is unavailable.
- The backbones are not connected.
- The router has blown a fuse.
- The hardware module is not attached firmly to the backplane.

Look at the GAME messages in the event log to determine the cause of the problem. If any of these events occurred and a slot is no longer functional, please call the Bay Networks Technical Solutions Center to report the problem.

Router Won't Boot

Troubleshoot the router as follows:

1. **If the router uses a flash memory card, make sure that you inserted it properly. See the appropriate router maintenance guide for instructions.**



Note: If you attempt to boot a router without a storage medium, or attempt to boot a router that does not have the proper router software image and configuration files, it will fail to boot and will stay in boot mode. The flash memory cards ship separately; you must install one unless the router is an older AN model.

2. **Wait five minutes.**

If the router's file system does not contain a configuration file named *config*, the router boots automatically with the *ti.cfg* file after five minutes. The *ti.cfg* file contains the minimum configuration required to boot the router and allow you to use the Technician Interface to access it. Make sure you name the configuration file *config*; then, reboot the router.

3. **If you recently installed the router software image, make sure it is correct for the router type.**

For detailed instructions on router software image compatibility, see *Upgrading Routers from Version 7-11.xx to Version 12.00*.

4. **If you set up the network to allow a BayStack or ASN router to netboot, see *Connecting ASN Routers to a Network* or *Configuring BayStack Remote Access*.**
5. **To diagnose a hardware problem with an ASN router, see Tables [3-1](#) and [3-2](#) and the instructions that follow. Otherwise, see the LED section of the router installation manual.**

Table 3-1. ASN Front-Panel Status Indicators

Status	Run LED	Boot LED	Diag LED
Initial power on	On	On	On
Diagnostics running	Flashes 1 second on, 1 second off	Off	Off
Booting	Off	On	Off
Normal operation	On	Off	Off*
Diagnostic failure (Testing detected at least one error)	Flashes 1 second on, 1 second off	Off	On ^a
Stack Packet Exchange (SPEX®) net module failure	Flashes 1 second on, 1 second off	Off	Flashes 1 second on, and alternates flashes with Run LED flashes

a. If the ASN boots with the Diag LED on, one or more of the connectors failed a diagnostic test. The ASN reports the failing connectors to the event log and brings up the interfaces on only those connectors that pass the diagnostic test.

Table 3-2. ASN Rear-Panel SPEX Module Status Indicators

LED	Meaning When On
FR	The SPEX net module is transmitting a frame.
FC	Flow Control is on. The SPEX net module uses Flow Control to reduce the rate of data transmission whenever there is congestion on the receiving end.

Troubleshoot an ASN as follows:

- a. **If the ASN is in a stack, make sure that the SPEX slot dial on the rear panel of each ASN points to a different slot ID. Turn the selector in either direction so that the arrow on the selector points to the ID you want to use (Figure 3-1).**

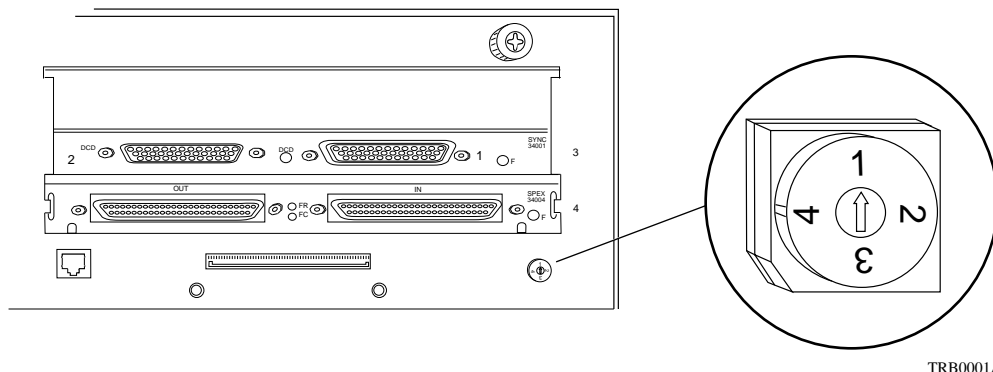


Figure 3-1. Verifying the Slot ID on an ASN

Make sure that the configuration matches the slot dial setting.

- b. **If the SPEX net module does not support hot-swap, make sure that a terminator plug connects to any unused ports labeled SPEX IN and SPEX OUT.**

Make sure that the thumbscrews on the terminator plug are tight.

If the ASNs are in a stack and do not support hot-swap, you must terminate the SPEX IN port of the first ASN and the SPEX OUT port of the last ASN. Make sure that, for the remaining ASNs in the stack, the SPEX OUT port of one ASN connects to the SPEX IN of the next ASN.



Note: For troubleshooting purposes, the ASN cables are long enough to skip one ASN in the stack.

Checking the Boot PROMs

Make sure that the boot PROM images are compatible with the router software image as follows:

1. **Enter the following command to display the software version of each boot PROM:**

get wfHwEntry.19.*

The number of the slot containing the boot PROM follows the dot (.) after the object name wfHwEntry.wfHwBootPromSource.

Example

```
$ get wfHwEntry.16.*
wfHwEntry.wfHwBootPromSource.2 = "int/12.00/freboot.exe"
wfHwEntry.wfHwBootPromSource.3 = "int/12.00/freboot.exe"
wfHwEntry.wfHwBootPromSource.4 = "int/12.00/freboot.exe"
wfHwEntry.wfHwBootPromSource.5 = "int/12.00/freboot.exe"
```

2. **See *Upgrading Routers from Version 7-11.xx to Version 12.00* to make sure that the boot PROM versions meet the software version requirements.**

Making Sure the Router Software Image Is Correct

Make sure that the router software image on the router is compatible with the type of router you are using. See *Upgrading Routers from Version 7-11.xx to Version 12.00* for a list of the router software image names and the associated router types.

Making Sure All Slots Use the Same Router Software Image and Configuration File

Different versions of router software image and configuration files in a router can cause serious problems. The best way to avoid these problems is to maintain consistency among the router software images in multiple flash memory cards. Also, make sure that, if you make a change to a configuration file on one flash memory card, you copy the file to any other flash memory cards that have a file with the same name.

If you specify the router software image and configuration files when booting the router, all processors boot with the specified router software image and configuration file.

If the router has more than one flash memory card, see the following sections to make sure that the router software image and configuration files in each processor are the same:

- [“Verifying That the Router Software Images in Each Processor Match”](#)
- [“Verifying That the Configuration Files in Each Processor Match”](#)

Verifying That the Router Software Images in Each Processor Match

To display the source of the router software images in each processor, enter the Technician Interface command **get wfHwEntry.28.*** or use the Statistics Manager Quick Get tool to display wfHardwareConfig > wfHwTable > wfHwActiveImageName.

Example

	Slot location of processor in router	Source volume of image in use	Name of image on the source volume
\$ get wfHwEntry.28.*			
wfHwEntry.wfHwActiveImageName.1	1	(nil)	
wfHwEntry.wfHwActiveImageName.2	2	2	bn.exe
wfHwEntry.wfHwActiveImageName.3	3	2	bn.exe
wfHwEntry.wfHwActiveImageName.4	4	2	bn.exe
wfHwEntry.wfHwActiveImageName.5	5	2	bn.exe

All settings for all processors must be the same.

TRB0003A

In this example, the processors in slots 2 through 5 are operating with the router software image named *bn.exe*, which came from the file system in volume 2. Here, slot 1 does not have a configuration because it does not contain a processor module.

If the slots are operating with router software images from different volumes, do the following:

1. **Display the directory for each slot and compare the file sizes of the router software images.**

If they are the same size, assume that the router software images are consistent and go to the next section, “[Verifying That the Configuration Files in Each Processor Match.](#)”

2. **Compare the file sizes with the backup router software image stored on the Site Manager workstation.**
3. **Determine which router software image you want to use.**

If you are not sure about the integrity of a router software image, do the following:

- a. **Use the Image Builder tool to customize an image.**
- b. **Back up the images on the flash memory cards.**
- c. **Remove the images from the flash memory cards.**
- d. **Compact the flash memory cards.**



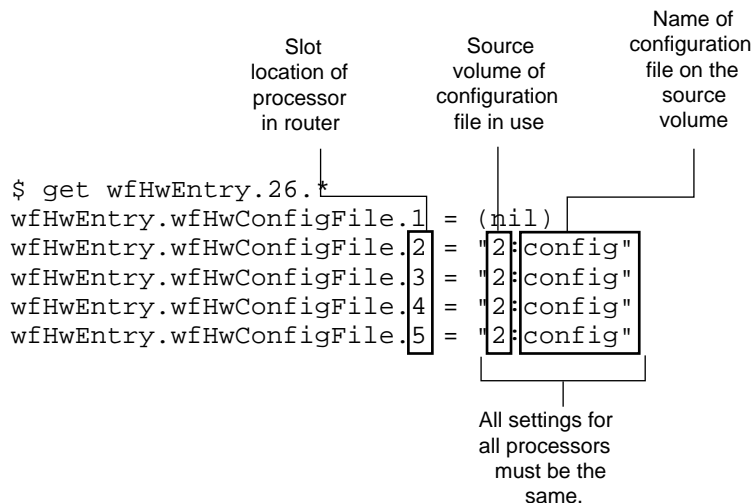
Caution: Do not interrupt the compaction.

- e. **Transfer the image you customized to the flash memory cards you want to use to store the image.**
 - f. **Reboot the router.**
 - g. **If this resolves the problem, stop here. If this does not resolve the problem, go to the next section, “[Verifying That the Configuration Files in Each Processor Match.](#)”**
4. **Back up the unwanted router software image.**
 5. **Remove the unwanted software image from the router’s file system.**
 6. **Determine which slots are running with the incorrect image and reset them.**

Verifying That the Configuration Files in Each Processor Match

To display the source of the configuration files in each processor, enter the Technician Interface command **get wfHwEntry.26.*** or use the Statistics Manager Quick Get tool to display wfHardwareConfig > wfHwTable > wfHwConfigFile.

Example



```
$ get wfHwEntry.26.*
wfHwEntry.wfHwConfigFile.1 = (nil)
wfHwEntry.wfHwConfigFile.2 = "2:config"
wfHwEntry.wfHwConfigFile.3 = "2:config"
wfHwEntry.wfHwConfigFile.4 = "2:config"
wfHwEntry.wfHwConfigFile.5 = "2:config"
```

All settings for all processors must be the same.

TRB0004A

In this example, the processors in slots 2 through 5 are operating with the configuration file named *config*, which came from the file system in volume 2.



Note: You can use a router software image from one volume and a configuration file from another.

If the slots are operating with configuration files from different volumes, do the following:

1. **Display the directory for each slot and compare the file sizes of the configuration files.**

If they are the same size, the configuration files are consistent. If they are not, continue with the remaining steps.

2. **Compare the file sizes with the backup configuration file stored on the Site Manager workstation.**

3. **Determine which configuration file you want to use.**
4. **Back up the unwanted configuration file.**
5. **Remove the unwanted configuration file.**
6. **Determine which slots are running with the incorrect configuration file and reset them.**

Lost Password (BN Routers)



Danger: Follow these instructions only if the router you are using is user serviceable. Routers that are not user serviceable, such as the AN, ASN, ANH, ARN, FN, LN, CN, and AFN, can cause electric shock. Call the Bay Networks Technical Solutions Center if you have lost a password and you have one of these types of routers.

When you create or change a password on a BN, the router distributes it to each FRE processor module, which in turn stores the new password on the local read-only memory (ROM) chip. If you remember the old password and want to change it, or you want to add password security for the first time, see the “System Administration” chapter in *Using Technician Interface Software* for instructions.

To replace a lost password, you need a FRE processor module that never operated in a router requiring a password, or one that operated in a router for which you know the password. Replace a lost password as follows:

1. **Disengage the thumb clips that secure all FRE processor modules to the slots, then pull each module slightly to disconnect it from the backplane. *Never completely remove more than one processor module from its slot.***



Danger: Never operate a router with more than one processor module completely removed from its slot.

2. **Remove one processor module from its slot.**
3. **Insert a FRE processor module that has never operated in a router that required a password, or one that operated in a router for which you know the password.**

4. **Insert the flash memory card containing the router software image and configuration file into the processor module.**
5. **Boot the router.**
6. **Engage the thumb clips of the other processor modules.**
7. **Wait for the processor modules to reset.**
8. **Enter the Technician Interface command `password [Manager / User]` to create or change the password.**

The new FRE processor module distributes the new password to the other processors, which then overwrite the old password.

No Space Left on Memory Card

When you delete a file on a flash memory card, the file management system makes the file inaccessible, but the file continues to use space on the card. Each time you store a file, the file system stores the file in the first unused space. Eventually, after you store and delete multiple files, the card runs out of usable space because the deleted files continue to take up space.

Use the Compact option in the File Manager Commands menu or enter the Technician Interface command **compact <volume>**: to free up space taken by deleted files.

For example, enter **compact 2**: to compact the files in volume 2. The file system copies all of the files to memory except for the deleted ones, erases the flash memory card, and copies the files back to the flash memory card.

When you copy a file on a flash memory card, the file system compares the size of the file with the amount of unused space on the flash memory card. If the file can fit in the unused space, the file system stores the file. If the file does not fit, the file system logs a message indicating the problem, but does not copy any portion of the file.

However, if the flash memory card runs out of space when saving a file from router memory or transferring a file using TFTP or FTP, the file system writes the file until it runs out of space, logs an `out of space` message, and then aborts the save or transfer operation. If this occurs, delete the partial file and compact the files on the flash memory card.

To view the status of a flash memory card, display its directory. The directory display shows the amount of available free space and how much of the free space is contiguous.

In the directory display, the available free space or free space column is the total number of bytes of unused space and bytes of space used by deleted files. The contiguous free space column is the number of bytes of unused space.

In order for the flash memory card to accommodate a file, the file's size must be less than or equal to the contiguous free space.

If the file you want to store is less than the available free space, but more than the contiguous free space, compact the existing files first. When you finish compacting files on a flash memory card, the contiguous free space matches the available free space.

Thus, if the directory display shows that the flash memory card has 1000 bytes of available free space and 1000 bytes of contiguous free space, all of its free space is available for storing files. If you store a file that is 100 bytes, you have 900 bytes of available free space and 900 bytes of contiguous free space. If you delete the file and display the directory, the display shows 1000 bytes of available free space, but only 900 bytes of contiguous free space. The 100-byte file remains on the flash memory card, even though you deleted it. Thus, only 900 bytes remain for storing additional files until you compact the existing files.

Memory or Buffer Problem

The router may have a memory or buffer problem if the log shows an out of resources or memalloc (memory allocation) error.

The router separates memory into two types:

- The router reserves global memory for all buffers.
These buffers store all incoming and outgoing traffic.
- The router reserves local memory for the router software image, the routing tables, and the forwarding tables.

The router software image includes both the operating system and executable software modules.

Thus, the amount of local memory available determines the maximum number of entries in a forwarding or routing table.

If the router has a shortage of local memory and an excess of global memory, you can use the configuration parameters in the Configuration Manager's Administration menu to increase available local memory. See Table 3-3 to determine how much memory is available for the type of processor in your router.

Table 3-3. Memory Available for Router Processor Types

Processor Type	Memory Type				Increment By Which You Can Allocate Memory
	Minimum Local	Maximum Local	Minimum Global	Maximum Global	
FRE-II	4 Mb	30 Mb	2 Mb	16 Mb	2 Mb
ACE32 4 Mb	2624 Kb (2.56 Mb)	3 Mb	1 Mb	1472 Kb (1.43 Mb)	1 Kb
ACE32 8 Mb	2624 Kb (2.56 Mb)	7 Mb	1 Mb	4 Mb	1 Kb
ACE32 16 Mb	2624 Kb (2.56 Mb)	12 Mb	1 Mb	4 Mb	1 Kb
AFN 4 Mb	2624 Kb (2.56 Mb)	3 Mb	1 Mb	1472 Kb (1.43 Mb)	64 Kb
AFN 16 Mb	2624 Kb (2.56 Mb)	12 Mb	1 Mb	4 Mb	64 Kb
AN/ANH	1868 Kb (1.82 Mb)	16204 Kb (15.82 Mb)	180 Kb	14516 Kb (14.17 Mb)	1 Kb

Determine how your processor currently uses local and global memory as follows:

1. **To determine how the slot in question divides memory into global and local memory, enter the following Technician Interface command:**

get wfKernParamEntry.*.<slot_no.>

<slot_no.> is the slot number of the processor module in the router. Use slot 1 if you have a BayStack router.

2. **To display how the router is using memory, enter the following Technician Interface command:**

get wfKernelEntry.*.<slot_no.>

The Technician Interface displays the following:

- How much memory is available
- The starting program counter (PC, which is the address location in memory) of the task

The Technician Interface displays each task as a PC code in the wfKernelEntry.wfKernelBufOwnerTask lines

- The number of buffers allocated for each task

Example

This example shows only the most important lines in the display.

```
$ get wfKernelEntry.*.2
wfKernelEntry.wfKernelSlot.2 = 2
wfKernelEntry.wfKernelMemorySize.2 = 23752016
wfKernelEntry.wfKernelMemoryFree.2 = 21139840
. . .
wfKernelEntry.wfKernelBufOwnerTask1.2 = "315910F4"
. . .
wfKernelEntry.wfKernelBufOwnerTask2.2 = "31619B04"
. . .
wfKernelEntry.wfKernelBufOwnerTask3.2 = "31619B04"
wfKernelEntry.wfKernelMemOwnerTask1.2 = "3002923E"
. . .
wfKernelEntry.wfKernelMemOwnerTask3.2 = "30081CF6"
. . .
```

3. To determine which protocols are running on the slot, enter the following Technician Interface command:

loadmap <slot_no.>



Note: Issue the **loadmap** command on the same slot on which you issued the **get wfKernelEntry.*.<slot_no.>** command. The order of the tasks changes each time you boot.

The **loadmap** display shows the protocols and other executable software modules running on the slot. Their associated starting PC codes are in hexadecimal format. The starting PC code of each wfKernelEntry attribute is a higher number than the PC code of its associated protocol.

Example

```
$ loadmap 2
```

```
-----
Loadmap from SLOT 2:
-----
--> arp.exe           0x31685720   0009784
--> vines.exe         0x315f47e0   0121448
--> ftp.exe           0x3164d6e0   0042868
--> tcp.exe           0x31657e70   0057776
--> tftp.exe          0x31666030   0020488
--> snmp.exe          0x3166b050   0030328
--> tn.exe            0x316726e0   0038424
--> ip.exe            0x31687d70   0182004
--> tms380.exe        0x3158ef80   0094428
--> hdlc.exe          0x31612260   0058496
--> dst.exe           0x315f3730   0004244
```

The column to the right of the display shows the number of bytes assigned to the module. If you convert the number of bytes to hexadecimal format and add it to PC code, the number equals the PC code of the next module in memory.

Determining which protocol owns a task can help you determine which protocols are using the most memory. To do this, compare the PC code of the `wfKernelEntry` attribute with the starting PC codes in the **loadmap** display. Determine which PC code in the display is the next higher number, compared with the number in the `wfKernelEntry` display, and which PC code is the next lower number. The protocol associated with the higher number owns the task.

Example

The following example shows another portion of the response to the **get wfKernelEntry.*.2** command:

```
$ get wfKernelEntry.*.2
. . .
wfKernelEntry.wfKernelMemOwnerTask6.2 = "315F7F08"
```

To make comparisons easier, the following illustration of the **loadmap** display reorganizes the entries by PC code. You can determine that the PC code 315F7F08 is a higher number than the PC code associated with the *vines.exe* software module, and that it is lower than the next highest PC code in the display, *hdlc.exe*. Therefore, the task is a VINES task.

```
$ loadmap 2
-----
Loadmap from SLOT 2:
-----
--> tms380.exe      0x3158ef80  0094428
--> dst.exe         0x315f3730  0004244
--> vines.exe       0x315f47e0  0121448
--> hdlc.exe        0x31612260  0058496
--> ftp.exe         0x3164d6e0  0042868
--> tcp.exe         0x31657e70  0057776
--> tftp.exe        0x31666030  0020488
--> snmp.exe        0x3166b050  0030328
--> tn.exe          0x316726e0  0038424
--> arp.exe         0x31685720  0009784
--> ip.exe          0x31687d70  0182004
```

If there is a significant number of lack-of-resource errors (more than 50/min), report the problem to the Bay Networks Technical Solutions Center.

Bad Forward Receive Buffer Checksum Errors

An event message beginning with `buf=` follows the message `bad forward receive buffer checksum`. See the bold text at the beginning of [Figure 3-2](#).

```
mm/dd/yy 12:35:56 141.122.57.1 5 GAME W "bad fwd receive buffer checksum"
mm/dd/yy 12:35:56 141.122.57.1 5 GAME D "buf=0x801c1b30 - 0x00000000
0x801ce400 0xffc0001 1 0x007c04a4 0x306da810 - xsum=0xd7781ec8

0x801da86c - 0x00050004 0x0022d300 0x76c00000 0x76c00000

0x801da87c - 0x8b51704d 0x30682854 0x0f00bbbb 0x0004000A

0x801da88c - 0xf300001c 0x8638002b 0xb9f1 1240 0xc0000000

0x801da89c - 0x20009000 0xa4850452 0x0002030c 0x31303030

0x801da8ac - 0x39303238 0x41343835 0x30313032 0x50534552

0x801da8bc - 0x5645525f 0x41353039 0x00000000 0x00000000

0x80"
```

TRB0002A

Figure 3-2. Finding the Slot Receiving Buffer Checksum Errors

Look at the number to the left of `GAME` on the first line of the error display. This is the number of the slot receiving the packet. In [Figure 3-2](#), slot 5 received the packet.

The number `0x0f00bbbb` indicates a backplane BofL packet, which is sent from one slot to another to determine whether the destination slot is running. If multiple BofL errors occur on the same sending or receiving slot, you may have a problem with the associated FRE processor.

Go to the appropriate section to determine which slot sent the backplane BofL packet:

- If the number 0x0f00bbbb is in the same location of your display as it is in Figure 3-2, go to “[Finding the Slot That Sent a Bad Backplane BofL Packet](#)”
- If the number 0x0f00bbbb is *not* in the same location, go to “[Finding the Slot That Sent a Bad Packet That Was Not a BofL Packet](#)”

Finding the Slot That Sent a Bad Backplane BofL Packet

Determine which slot sent the BofL packet that failed as follows:

1. **Find the number 0x0f00bbbb.**
2. **Find the number to the right of the number 0x0f00bbbb.**

In Figure 3-2, this number is 0x0004000A.

3. **Convert the last four digits of that number to decimal.**

In the following example, slot 10 sent the bad backplane BofL packet:

0x000A = 10

4. **Call the Bay Networks Technical Solutions Center and describe the problem.**

Depending on whether the slot sending or receiving the packet is always the same, you may need to replace the processor.

Finding the Slot That Sent a Bad Packet That Was Not a BofL Packet

Find the number of the slot that sent the bad packet by looking at the hexadecimal number that is in the same position as the bold number in Figure 3-3.

```
mm/dd/yy 04:58:56 141.122.57.1 4 GAME W "bad fwd receive buffer checksum"
mm/dd/yy 04:58:56 141.122.57.1 4 GAME D "buf=0x801da800 - 0x00000000
0x801ce400 0xffc00011 0x007c04a4 0x306da810 - xsum=0xd7781ec8
0x801da86c - 0x00050004 0x0022d300 0x76c00000 0x76c00000
0x801da87c - 0x8b51704d 0xa0000012 0x221a090b 0x00000121
0x801da88c - 0xf300001c 0x8638002b 0xb9f11240 0xc0000000
0x801da89c - 0x20009000 0xa4850452 0x0002030c 0x31303030
0x801da8ac - 0x39303238 0x41343835 0x30313032 0x50534552
0x801da8bc - 0x5645525f 0x41353039 0x00000000 0x00000000
0x80 "
```

TRB0005A

Figure 3-3. Finding the Slot Number When the Buffer Checksum Message Does Not Reference a Backplane BofL Packet

In the following example, the hexadecimal number in question is the 0xa000 portion of the number 0xa0000012. Convert the number to its binary equivalent.

0xa000 = 1010 0000 0000 0000

In the binary representation of the number, a value of 0 means that the slot *did not* originate the message; a value of 1 means that the slot did originate the message. Ignore the leftmost digit. The digit to the right of the leftmost digit is the value for slot 1, the next digit to the right is the value for slot 2, the next digit to the right is the value for slot 3, and so on. The rightmost digit is meaningless because the router can only have 14 slots. In this example, slot 2 sent the message that failed.

Call the Bay Networks Technical Solutions Center and describe the situation. Depending on whether the slot sending or receiving the packet is always the same, you may need to replace the FRE processor.

Fault Message

If a software entity experiences a fault and fails to recover, do the following:

1. **Disable and reenable the port.**

Watch the event log. Stop here if the software entity recovers.

2. **Reset the slot.**

Watch the event log. Stop here if the software entity recovers.

3. **Press the Reset button on the front panel for no more than one second.**

This initiates a warm-start procedure, which will keep the log intact.



Caution: Avoid using the **diags** command to boot a router after it has gone down. If you do, or if you remove and reinstall power, the diagnostics software overwrites the log. This prevents you from accessing the log to determine the cause of the problem.

Watch the event log. Stop here if the software entity recovers.

4. **Save the log to a file and use FTP or TFTP to transfer it to the Bay Networks host. Or, set the router up for modem access so that Bay Networks can dial in and look at it.**

Go to Chapter 8 for instructions.

5. **Call the Bay Networks Technical Solutions Center to report the problem.**

Chapter 4

Troubleshooting a Physical Media Problem

This chapter describes how to solve physical media problems. It assumes that you have already determined the scope of your problem, as described in Chapter 2.

Topic	Page
Making Sure the Link Module Is Working	4-1
Determining the Media-Specific State	4-1
Troubleshooting the Cable Connection	4-3

Making Sure the Link Module Is Working

Refer to the event log to make sure that the link module and ports are enabled. If they are not, examine the log messages for the slot in question to determine whether they were disabled or were never enabled, and why.

Determining the Media-Specific State

Use the Statistics Manager Quick Get tool or the Technician Interface to check the media-specific state of the connector in question. Using the Quick Get tool, choose wfLine > wf<MEDIA>Table to retrieve the State attribute. Or, using the Technician Interface, enter the following command:

get <object>.3.<slot_no>.<connector_no>

<object> is one of the following: wfCSMACDEntry, wfSyncEntry, wfT1Entry, wfE1Entry, wfTokenRingEntry, wfFddiEntry, or wfHssiEntry.

The numeric identifier of the State attribute for these objects is 3.

For example, enter **get wfCSMACDEntry.3.1.4** to display the state of Ethernet in slot 1, connector 4.

You can use the wildcard character (*) to display the states of all connectors of a particular type on a slot, or all connectors of a particular type on the entire router. For example, enter **get wfCSMACDEntry.3.*** to display the state of all Ethernet connectors on the router.

Example

```
$ get wfCSMACDEntry.3.*
wfCSMACDEntry.wfCSMACDState.1.1 = 1
wfCSMACDEntry.wfCSMACDState.1.2 = 1
wfCSMACDEntry.wfCSMACDState.1.3 = 1
wfCSMACDEntry.wfCSMACDState.1.4 = 1
```

Table [4-1](#) describes the values of the State attribute.

Table 4-1. State Attribute Values

Value	Meaning of State Attribute						
	CSMA/C D	Sync	T1	E1	Token Ring	FDDI	HSSI
1	up	up	up	up	up	up	up
2	down	down			down	down	LMI wait
3	initializing	initializing	initializing	initializing	initializing	initializing	BofL wait
4	not present	wait	not present	not present	not present	not present	CA wait
5		not present					initializing
6		DSR wait					not present
7		hold down					
8		remote loop					

Respond to the State attribute values as follows:

1. **If the state of the interface in question is up, check the statistics associated with that layer.**

If the statistics show that the media is OK, go to Chapter 6.

2. **If the state is not present, the dynamic loader did not load the driver (lower-layer protocol) on the slot. Make sure the link or net module and port are up. Then, make sure the driver runs on the slot in the configuration of the router.**
3. **If the state is down, check the log to determine the reason, as follows:**
 - a. **Save the log.**
 - b. **Issue the `clearlog` command.**
 - c. **Use the Configuration Manager to set the Enable parameter to Disable, or use the Technician Interface to set the Enable attribute to 2.**
 - d. **Use the Configuration Manager to set the Enable parameter to Enable, or use the Technician Interface to set the Enable attribute to 1.**
 - e. **View the log.**
 - f. **If the state is not up, test the cable and the transceiver.**
4. **If the cable and transceiver are OK, use Packet Capture to test the reception and transmission of data as it passes through the cable. See Appendix B for instructions.**

Troubleshooting the Cable Connection

Check the cable that carries the data as follows:

1. **If a problem occurred after connecting a new cable, make sure it is the proper cable for the application you are using.**

See the *Cable Guide* for information.

2. **Make sure that both ends of the cable are firmly connected to the proper interfaces.**



Note: Do not use the connector position in one link module to determine the position of another. Interface 1 of one type of link module may be on the left side, and interface 1 of another type may be on the right side. Verify the connection by looking at the connector number on the link module.

3. **Check the LEDs on the rear panel of the router.**

The green transceiver light comes on when the cable is secure.

If you hot-swapped a link module or reset the slot, the associated red fail LED remains on until you run diagnostics on that slot. This condition does not necessarily indicate a problem. However, if you run diagnostics on a slot and the red fail LED remains on for more than a few minutes, call the Bay Networks Technical Solutions Center.



Caution: Connect only cables that support hot-swap to connectors that support hot-swap. Also, connect only cables that do not support hot-swap to connectors that do not. Otherwise, damage to the board may occur.

4. **If the state of the connector is down, replace the cable.**

Determine whether the problem is with the cable or the port by replacing the cable with a cable that you know is good.

5. **Perform local and remote loopback tests during network downtime, or on ports that are not in use.**



Caution: Do not do loopback testing during network production time if the bridge is operating on the port.

You can also loop back PPP lines; however, if you configured them with a password, you must configure them in promiscuous mode first.

If you are accessing a DTE/DCE line with promiscuous mode off, the port will not increment the reception statistics.

If the connection is FDDI or ATM Rx and Tx:

- a. **Make sure you have cabled ports A and B correctly.**
- b. **Try looping port A back to port B to test for port failure.**

If the Tx and Rx LEDs light, the ports and cable are OK.

- c. **Check the event log to make sure that the router brings the ring up and marks the circuit as active.**
- d. **If the loopback test fails, try a different fiber cable. Then, try replacing the link module.**



Note: Multimode fiber is orange, and single-mode fiber is yellow. The different fibers require different interface modules.

Chapter 5

Troubleshooting a Data Link Layer Problem

This chapter describes how to solve data link layer problems. It assumes that you have already determined the scope of your problem, as described in Chapter 2.

Topic	Page
Troubleshooting an ATM Connection	5-2
Troubleshooting an Ethernet Connection	5-9
Troubleshooting a FDDI Connection	5-14
Troubleshooting a Frame Relay Connection	5-17
Troubleshooting an MCT1 Connection	5-20
Troubleshooting a Synchronous Connection	5-22
Troubleshooting a Token Ring Connection	5-27
Troubleshooting Other Data Link Layer Protocols	5-29

Troubleshooting an ATM Connection

This section assumes that you have isolated a problem to an ATM interface. If not, refer to Chapter 2 to determine whether these instructions apply.

How you troubleshoot ATM depends on your ATM configuration. First, follow the steps in the section “[Interface Problems](#).” Then, see “[Troubleshooting ATM LANE](#)” on [page 5-7](#), if applicable.

Interface Problems

Troubleshoot an ATM connection as follows:

1. **Use the Events Manager or the Technician Interface to enable extended debugging for the wfAtmInterface MIB objects.**

The Technician Interface command is as follows:

```
g wfAtmInterfaceConfEntry.wfAtmInterfaceDebug.*
```

2. **Filter the log to display only messages from the ATM entity running on the slots experiencing the problem.**

The Technician Interface command is as follows:

```
log -fftwid -eATM -eATMINTF -s<slot_no.>
```

For example, if you are filtering events from slots 3 and 4, enter the following command:

```
log -fftwid -eATM -eATMINTF -s3 -s4
```

3. **Use the Events Manager or the Technician Interface to display the attributes associated with the MIB objects in [Table 5-1](#).**

Table 5-1. First Set of ATM Interface MIB Objects to View

MIB Object	Description	Quick Get Path
wfAtmInterfaceConfEntry ^a	Shows the configuration of the ATM port, including the aggregate cell rate and maximum number of VCs on the port.	wfLine > wfAtmInterfaceGroup > wfAtmCommonGroup > wfAtmInterfaceConfTable
wfAtmVclConfEntry	Shows the VCL configuration, including the mode (direct, group, or hybrid) and the cell rates (burst, sustainable, or peak).	wfLine > wfAtmInterfaceGroup > wfAtmCommonGroup > wfAtmVclConfTable
wfAtmVclStatsEntry	Shows the number of cells received and transmitted, and the number of frames dropped on specific VPIs or VCIs.	wfLine > wfAtmInterfaceGroup > wfAtmCommonGroup > wfAtmVclStatsTable

a. The instance ID associated with this object is the line number.

4. **Redisplay the MIB objects in [Table 5-1](#) after 1 minute; then, compare the values to determine which errors are currently occurring.**

[Table 5-2](#) lists specific attributes to check and describes possible actions.

Table 5-2. ATM Interface Attributes for Troubleshooting

Attribute	Description	Action
wfAtmVclRcvCrcErrs	Shows the number of errors due to line noise.	Check for defective fiber media.
wfAtmVclRcvMaxLenExceedErrs	Shows the number of packets coming from the ATM code and sent to the driver for transmission that exceeded the maximum transmission unit (MTU) configured on the VCL.	Check the configuration of the MTU, and consider increasing the MTU.
wfAtmVclRcvInvalidLenErr	Shows the number of segmentation and reassembly (SAR) frames that contain a length error after protocol data unit (PDU) reassembly.	Check dropped-frame statistics; then, locate the dropped frames by checking the path of cells through the network.

5. Use the Events Manager or the Technician Interface to display the attributes associated with the MIB objects in [Table 5-3](#).

Table 5-3. Second Set of ATM Interface MIB Objects to View

MIB Object	Description	Quick Get Path
wfAtmAlcDrvEntry	Shows how much data the link module is transmitting	wfLine > wfAtmInterfaceGroup > wfAtmLinkModule > wfAtmAlcDrvEntry
wfAtmAlcCopErrorEntry	Shows physical errors such as link delineation errors	wfLine > wfAtmInterfaceGroup > wfAtmLinkModule > wfAtmAlcCopErrorEntry
wfAtmAlcCopDataPathEntry ^{ab}	Shows the ATM coprocessor buffer utilization, the number of cells received and transmitted, and the number of dropped (clipped) frames	wfLine > wfAtmInterfaceGroup > wfAtmLinkModule > wfAtmAlcCopDataPathEntry

a. The instance ID associated with this object is the line number.

b. There are no statistics available on the types of cells received and transmitted; the value is always 0.

6. Redisplay the MIB objects in [Table 5-3](#) after 1 minute; then, compare the values to determine which errors are currently occurring.

If applicable, see one of the following sections:

- [“Dropped Frames”](#)
- [“ATM VC Mod Failed Message”](#)
- [“Upper-Layer Protocols Failing to Pass Packets”](#)
- [“PVC Problems”](#)

Dropped Frames

Troubleshoot dropped frames as follows:

1. Use the Events Manager or the Technician Interface to display the attributes in [Table 5-4](#).

Table 5-4. Troubleshooting Dropped Frames

Attribute	Description
wfAtmAlcDrvEntry.wfAtmAlcXmtPacketClips	Shows whether the ATM port is dropping frames because of congestion on the outgoing queue
wfAtmAlcCopDataPathEntry.wfAtmAlcCopRcvClipPackets	Shows whether the ATM port is dropping frames because of congestion on the incoming queue

2. Redisplay the attributes in [Table 5-4](#) after 1 minute; then, compare the values to determine which errors are currently occurring.
3. Determine which upper-layer protocols configured to run on the same port are receiving data.
4. Use Packet Capture and a network analyzer to determine which type of data is on the line.

ATM VC Mod Failed Message

If the message `ATM VC mod failed` appears, the VC request to the driver failed. The message `VC ATM add failed` usually appears next. Do the following:

1. Check the VC definition in the configuration file and make sure that you defined the ATM adaptation layer (AAL) type as AAL 5.
2. Determine whether an oversubscription of the port cell rate occurred.
3. Make sure you used a VCI number greater than 32.

4. Match the error code in the message to the Error Code column in Table 5-5, and follow the associated instructions.

Table 5-5. Error Codes in the “ATM VC mod failed” Log Message

Error Code	Meaning	Instructions
ATM_ERR_BAD_VC	The driver is already using the VPI/VCI.	Use a different channel.
ATM_ERR_NO_RESOURCE	The bandwidth is insufficient to satisfy the request.	Lower the cell rates.
ATM_ERR_NO_VC_AVAIL	The maximum number of VCs are already in use.	Increase the maximum number of VCs.
ATM_ERR_COP_ERR	The coprocessor returned an error.	Document the error and call the Bay Networks Technical Solutions Center.

Upper-Layer Protocols Failing to Pass Packets

If the interfaces are receiving and transmitting frames, but the upper-layer protocols are failing to pass packets to ATM, do the following:

1. Find the message indicating that Data Path created a gate for the VC.

The message looks like this:

```
# 316: mm/dd/yy 14:57:42.417 DEBUG SLOT 3 DP Code: 23
Adding VC gate w/GH 0x627e to cct 3
```

The abbreviation w/GH stands for “with gate handle.” A gate handle is the logical address of a process.

2. Check the remaining log messages to make sure that the operating system did not kill this gate.
3. Verify that payload scrambling is either disabled or enabled on both sides of the ATM connection.

If there is a mismatch, the router will receive data and there will be no errors, but data will disappear. Scrambling is enabled on the router by default and cannot be disabled on non-DS3 ARE ATM interfaces, but can be enabled or disabled on FREII/FRE 60 ATM interfaces.

PVC Problems

For PVC problems, do the following:

1. **If the connecting switch does not support signaling, verify that signaling is disabled.**
2. **Check the log for failed to register messages.**
 This message usually indicates an oversubscribed interface. Add the peak cell rate (PCR) and sustainable cell rate (SCR) values of each PVC to verify that the combined value does not exceed the cell rates you have configured on the interface.
3. **If the PVC terminates at a non-Bay Networks IP device, define an adjacent host entry using the outgoing VPI/VCI number of the device as the MAC address.**
4. **Using the VCL MIB objects, verify the configured cell and frame statistics for each VC.**
5. **If the interface is running LLC/SNAP encapsulation, check the wfAtmMpeEntry MIB object for PID errors.**
6. **Verify that the PVC is not a termination point for a C100 connection (such as C100 Turbo or Circuit Saver).**

Troubleshooting ATM LANE

This section assumes that you have isolated a problem to the ATM LAN emulation (LANE) protocol. Troubleshoot ATM LANE problems as follows:

1. **Use the Events Manager or the Technician Interface to enable extended debugging in the wfAtmLec MIB objects.**

The Technician Interface command is as follows:

g wfAtmLecConfigEntry.29.3

2. **Filter the log to display messages of all severity levels for the slots experiencing the problem.**

Enter the following Technician Interface command:

log -fftwid -eATM -eATM_SIG -eATM_LE -s<slot_no.>

3. Use the Events Manager or the Technician Interface to display the attributes associated with the MIB objects in [Table 5-6](#), and take the appropriate action.

Table 5-6. ATM LANE MIB Objects to View

MIB Object	Description	Action
wfAtmSigEntry	Shows the status of ATM signaling	Verify that Signaling software is up.
wfAtmIlmiEntry	Shows the status of ILMI	Verify that ILMI software is up.
wfAtmNetPrefixEntry	Shows the status of the network prefix	Verify that the router received its network prefix from the switch.
wfAtmLecStatusEntry	Shows the status of all LAN emulation clients (LECs)	Check the current state of the LEC process in the wfLecInterfaceState attribute. Values are as follows: <ul style="list-style-type: none"> • initial (1) • lecsconnect (2) • configure (3) • join (4) • reg (5) • busconnect (6) • operational (7)
wfAtmServiceRecordEntry	Shows the status of LANE service records	<ol style="list-style-type: none"> 1. Verify the configured ATM suffix (ESI or Selector). 2. Determine the complete 20-byte ATM address. 3. If MIB attribute #10 is zero (0), the service record did not register its address; check the log. 4. If MIB attribute #9 is all zeros, autogeneration is enabled.
wfAtmLecStatisticsEntry	Shows information about all of the LANE control packets that this service record has received or transmitted	Check the ATM_LE log for the message LE_ARP timeout or LE_ARP no response.
wfAtmLecServerVccEntry ^a	Shows which LANE control SVCs are operational and their VPI/VCI values	
wfAtmLecConfigEntry	Shows configuration values for LEC and LAN emulation configuration server (LECS) attributes	Verify that the LEC and LECS have the same value for the ELAN Name attribute. Note that emulated LAN (ELAN) names are case-sensitive.
wfAtmLecArpEntry	Shows ARP information	Verify the LANE ARP cache.

a. The instance ID associated with this object is the circuit number of the service record.

Troubleshooting an Ethernet Connection

This section assumes that you have isolated a problem to an Ethernet connection. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot an Ethernet connection as follows:

1. **Filter the log to display only messages from the CSMA/CD entity running on the slots experiencing the problem.**

The Technician Interface command is as follows:

log -fftwid -eCSMACD -s<slot_no.>

Example

If you are filtering events from slots 3 and 4, enter the following command:

log -fftwid -eCSMACD -s3 -s4

2. **If only one port on the slot is reporting errors, try switching out the transceiver/hub port that the router is connected to, or the actual cable that connects the router to the transceiver or twisted-pair connection.**

If the problem persists, verify the configuration of the Ethernet port. Then, switch the problem connection to another Ethernet port. If the errors stop occurring, you may have a bad Ethernet port. You should either replace the link module or call the Bay Networks Technical Solutions Center.

3. **Use the Technician Interface to look at the values of the following attributes in the wfCSMACDEntry MIB object. Or, access them using the Quick Get path wfLine > wfCSMACDTable.**

- wfCSMACDDelete

This shows whether you configured CSMA/CD (1) or whether you did not (2).

- wfCSMACDEnable

This shows whether CSMA/CD is enabled (1) or disabled (2) on the line.

- wfCSMACDState

This shows whether CSMA/CD is up (1), down (2), initializing (3), or not present (4).

- `wfCSMACDOctetsRxOk`

This shows the number of bytes received without error.

- `wfCSMACDFramesRxOk`

This shows the number of frames received without error.

- `wfCSMACDOctetsTxOk`

This shows the number of bytes transmitted without error.

- `wfCSMACDFramesTxOk`

This shows the number of frames transmitted without error.

- `wfCSMACDDeferredTx`

This shows the number of deferred transmissions. The Ethernet port detected a frame transmitting on the segment when it was preparing to transmit another frame. This is not an error, but an indication of a busy segment. If this statistic changes rapidly, determine why the segment is so busy.

- `wfCSMACDLateCollnTx`

This shows the number of late collisions transmitted. A late collision transmission is a collision that takes place after the router transmits the first 64 bytes of a frame. The Ethernet controller chip (ILACC, Integrated Local Area Communications Controller) does not retransmit the frame. The length of the Ethernet cable exceeds the specified length. Use a cable length that complies with the IEEE 802.3 specification.

Late collisions may indicate that the Ethernet LAN exceeds the length of the IEEE 802.3 specification.

- `wfCSMACDExcessvCollnTx`

This shows the number of excessive collisions. The software declares an excessive collision when 16 successive attempts to transmit a frame fail because each attempt results in a collision. The router discards the frame and adds one to the error count.

This is an indication of an overloaded segment with possible data storms. Analyze this segment in order to determine what type of traffic is causing the problem.

- **wfCSMACDBablErrorTx**

This shows the number of frames transmitted that were larger than 1518 octets. BablErrorTx stands for babbling transmitter errors. Despite declaring an error, the Ethernet controller chip transmits the packet in its entirety.

Disable and enable the port and check the log for errors.

- **wfCSMACDLcarTx**

This shows the number of loss-of-carrier errors, which is the number of times the port on the router lost the carrier connection during transmission to an external transceiver device. After carrier loss, the Ethernet controller chip continues to transmit the frame and the CSMACD entity logs an event. The controller chip does not retransmit the frame.

This could indicate a bad transceiver cable, bad transceiver, or bad hub port.

- **wfCSMACDFcsErrorRx**

This shows the number of frames dropped upon receipt over this CSMA/CD line because the Ethernet controller chip detected a check sequence (checksum) error. The cause is usually physical.

Make sure the cables are firmly connected. Test the cables.

- **wfCSMACDAlignErrorRx**

This shows the number of frames dropped upon receipt over this CSMA/CD line because the Ethernet controller chip detected a frame alignment error. An incoming frame contained a non-integer multiple of eight bits and a checksum error. If an incoming frame contains a non-integer multiple of eight bits, but does not have a checksum error, it does not increase this count. When this count is incremented, the cause is usually physical.

Make sure the cables are firmly connected. Test the cables.

- **wfCSMACDLackRescErrorRx**

This shows the number of receiver lack-of-resource errors. It indicates the number of times the router dropped packets it received because of a lack of buffers. Some lack-of-resource errors are likely, especially when the router boots. If this number increases to a high rate (such as 15/minute) for an extended period, it may indicate a problem.

Check the `wfKernelEntry` for the slot where the problem is occurring to determine whether buffers are available or whether something on the network is preventing the router from updating its buffer lists. To do this, use the command **get wfKernelEntry.*.<slot>**. For example, enter the command **get wfKernelEntry.*.2**. The router reports the number of available buffers in slot 2.

Check for protocol storms (for example, from IP RIP, IPX RIP, and SAP, and learning bridge reconverging). If no buffers are available, check the configuration of the line and the line utilization.

Increase the `wfCSMACDCfgRxQueueLength` to 64 and see if that helps alleviate the problem.

- **wfCSMACDTooLongErrorTx**

This shows the number of frames received that exceed 1518 octets. The router drops the frames because of a lack of space on the transmission queue (Tx). Some lack-of-resource errors are likely, especially when the router boots. If this number increases to a high rate (such as 15/minute) for an extended period, it may indicate a problem.

Check the `wfKernelEntry` for the slot where the problem is occurring to determine whether buffers are available or whether something on the network is preventing the router from updating its buffer lists. To do this, enter the command **get wfKernelEntry.*.<slot>**. For example, enter the command **get wfKernelEntry.*.2**. The router reports the number of available buffers in slot 2.

Check for protocol storms (for example, from IP RIP, IPX RIP, and SAP, and learning bridge reconverging). If no buffers are available, check the configuration of the line and the line utilization.

Increase the `wfCSMACDCfgRxQueueLength` to 64 and see if that helps alleviate the problem.

- **wfCSMACDMerr**

This shows the number of Ethernet controller chip memory errors. The controller chip declares an error when it fails to access memory within 1512 clock ticks of asserting its data strobe signal. After declaring a memory error, the controller chip reinitializes. Go to “Memory or Buffer Problem” in Chapter 3.

- **wfCSMACDCerr**

This shows the number of Ethernet controller chip collision detections. This is meaningful only if the attached transceiver or hub device implements an SQE (signal quality error, or Ethernet heartbeat) test as defined in the IEEE 802.3 specification. SQE specifies the periodic assertion of the transceiver's collision detection circuitry during down periods, and tests the integrity of the controller chip/transceiver connection.

If the transceiver or hub device does not implement SQE, the value (0 or 1) is irrelevant.

If the transceiver or hub device implements SQE:

- 0 indicates successful completion of the test.
- 1 indicates that the SQE test failed. In this case, CSMA/CD logs an event noting SQE loss and verifies the integrity of the fuse. If the fuse is the problem, CSMA/CD logs another event and disables service to the line. If the fuse is OK, CSMA/CD retains service to the line.

- **wfCSMACDTxClipFrames**

This shows the number of frames clipped in the driver's transmission routine due to transmission congestion. Check for the type of data that is transmitting. Determine whether a broadcast storm is disrupting the network, or whether the traffic is too heavy for the segment.

- **wfCSMACDRxReplenMisses**

This shows the number of packet-buffer misses while attempting to replenish the driver reception ring. Another entity is using all of the available buffers. Go to "Memory or Buffer Problem" in Chapter 3.

- **wfCSMACDUnAlignedFrames**

This shows the number of non-word-aligned frames received for transmission. A non-word-aligned frame means that the starting address of the data in memory is not an even number. Some protocol implementations in the router create non-word-aligned frames.

If the Ethernet controller is *not* a Quad Ethernet (QENET), you can ignore this attribute. If the Ethernet controller is a QENET, check for underflow errors or corrupted frames. (This usually occurs only when you configure three or more ports on the QENET.)

If underflow errors or corrupted frames occur, enable the attribute `wfCSMACDAlignmentMode`, which determines whether the software aligns the frame on a word boundary before giving it to the QENET.

- `wfCSMACDLateCollnRx`

This shows the number of late collisions received. A late collision reception is a collision that takes place after the router receives the first 64 bytes of a frame. The length of the Ethernet cable exceeds the specified length. Use a cable length that complies with the IEEE 802.3 specification.

Troubleshooting a FDDI Connection

This section assumes that you have isolated a problem to a FDDI connection. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot a FDDI connection as follows:

1. **Filter the log to display only messages from the FDDI entity running on the slots experiencing the problem.**

The Technician Interface command is as follows:

```
log -fftwid -eFDDI -s<slot_no.>
```

Example

If you are filtering events from slots 3 and 4, enter the following command:

```
log -fftwid -eFDDI -s3 -s4
```

2. **Use the Technician Interface to look at the values of the following attributes in the `wfFddiEntry` object. The `get` command is next to the attribute name. Or, use the `wfLine > wfFddiTable Quick Get` path to access them.**

- `wfFDDIOverrunRx` (**`get wfFddiEntry.16.*`**)

This shows the number of frames received with internal overrun errors. The FDDI System Interface (FSI) chip set became overloaded and dropped packets.

- **wfFDDIRingOverrunRx (get wfFddiEntry.21.*)**

This shows the number of logical link control (LLC) reception ring overrun events. These errors are equivalent to lack-of-resource errors on a synchronous or Ethernet port. Each error indicates one lost packet. Troubleshoot a problem with reception ring overruns as follows:

- Enter the following command to verify how many buffers are currently free in the slot:

get wfKernelEntry.*.<slot>

- Go to “Memory or Buffer Problem” in Chapter 3 if you need an explanation of the memory issues.
- Increase the size of the reception queue by setting the wfFddiEntry.43 attribute (wfFDDICfgRxQueueLength). The maximum setting is 255.

- **wfFDDITxClipFrames (get wfFddiEntry.40.*)**

This shows the number of dropped (clipped) frames that the router could not add to the driver’s transmission routine because of transmission congestion. Determine what type of data is overrunning the transmission port by using a network analyzer or the Packet Capture utility.

Enter the following command to verify how many buffers are currently free in the slot:

get wfKernelEntry.*.<slot>

Go to “Memory or Buffer Problem” in Chapter 3 for an explanation of the memory issues.

Increase the size of the transmission queue by setting the wfFddiEntry.42 attribute (wfFDDICfgTxQueueLength). The maximum setting is 255.

3. Enter the Technician Interface command get wfFddiSmtEntry.9.* or use the Quick Get path wfLine > wfFddiGroup > wfFddiSmtGroup > wfFddiSmtTable > wfFddiSmtCfState.

This shows the connection of the station to the ring. The codes are as follows:

- 1 = isolated
- 2 = wrap S
- 3 = wrap A
- 4 = wrap B

This state indicates that ports A and B connect to two different concentrators that connect to the same ring.

- 5 = wrap AB
- 6 = through

This is the normal, non-wrap operating state for a dual-attached station.

- 7 = local A
- 8 = local B
- 9 = local AB
- 10 = local S
- 11 = cwrap A

This state indicates that FDDI wrapped port A of the FDDI link or net module because port B is not receiving data.

Make sure that the port B cable is not disconnected and that the port is functional. One of the two fibers leading into port B may be broken. Troubleshoot the cable.

- 12 = cwrap B

This state indicates that FDDI wrapped port B of the FDDI link or net module because port A is not receiving data.

Make sure that the port A cable is not disconnected and that the port is functional. Troubleshoot the cable.

4. **Use the Technician Interface to look at the values of the following attributes in the wfFddiMacEntry object. The get command is next to the attribute name. Or, use this Quick Get path to access them: wfLine > wfFddiGroup > wfMacGroup > wfFddiMacTable**

- wfFddiMacUpstreamNbr (**get wfFddiMacEntry.4.***)

This shows the MAC address of the upstream neighbor in the ring. Use it to determine whether the router wrapped the ring.

- wfFddiMacDownstreamNbr (**get wfFddiMacEntry.5.***)

This shows the MAC address of the downstream neighbor in the ring. Use it to determine whether the router wrapped the ring.

Troubleshooting a Frame Relay Connection

This section assumes that you have isolated a problem to a Frame Relay connection. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Filter the log to display only messages from the Frame Relay entity running on the slots experiencing the problem. The Technician Interface command is as follows:

```
log -fftwid -eFR -s<slot_no.>
```

Example

If you are filtering events from slots 3 and 4, enter the following command:

```
log -fftwid -eFR -s3 -s4
```

Refer to the symptoms described in the sections that follow:

- [“Log Messages from Frame Relay Indicate Circuit Is Down”](#)
- [“Frame Relay Switch Keeps Marking the Circuit as Down”](#)
- [“Frame Relay Circuit Up, but Protocol Data Is Not Transmitting”](#)
- [“PVC Transmitting, but Not Receiving”](#)
- [“Frame Relay Configured with LMI Invokes an Xoff State”](#)

Log Messages from Frame Relay Indicate Circuit Is Down

Troubleshoot as follows:

1. **Check the Sync interface statistics to determine whether the Sync interface is receiving and sending traffic.**
2. **Make sure the status message timeout configurations of the switch and the router are the same.**
3. **Determine whether the virtual circuit (VC) and synchronous interface are receiving packets.**
4. **Make sure the VC is enabled.**

Frame Relay Switch Keeps Marking the Circuit as Down

Troubleshoot as follows:

1. Check the polling interval configuration on the switch and the router.
2. Check the log for any events issued by Frame Relay to determine the status of the Frame Relay link.

Frame Relay Circuit Up, but Protocol Data Is Not Transmitting

Troubleshoot as follows:

1. Check the data link control identifier (DLCI) protocol configuration.
2. Check the routing tables for the correct routing information.
3. Check whether this problem is affecting all protocols or a single protocol.
4. Examine the FrVcError statistics to determine whether the router is dropping any packets.
5. Display the values of the VcCircuitEntry object to determine whether the switch initiated flow control.
6. Display the wfFrVCircuitEntry values and check the number of forward explicit congestion notifications and backward explicit congestion notifications (FECNs/BECNs).

The attribute names for FECNs and BECNs are wfFrCircuitReceivedFECNs and wfFrCircuitReceivedBECNs. The FECNs and BECNs indicate congestion on the network.

PVC Transmitting, but Not Receiving

If the log indicates that the permanent virtual circuit (PVC) is active, and the statistics indicate that it is transmitting but not receiving, do the following:

- Make sure that the Frame Relay switch on the remote side of the link supports the A-bit.
- The switch sends the A-bit to the router to indicate that it is up and active. If the switch does not support the A-bit, the router has no way of determining whether the remote side of the link is down, and thus fails to disable the associated PVC.
- Determine whether the switch can loop back any data.

Frame Relay Configured with LMI Invokes an Xoff State

If a Frame Relay switch exceeds buffer thresholds and sends an R-bit, the router invokes an Xoff state. Xoff is equivalent to a disabled VC. The router disables the DLCI/VC that received the R-bit. If the DLCI that received the R-bit is in direct mode, the router also disables all the upper-layer protocols associated with the DLCI. If the DLCI is in group mode, the upper-layer protocols continue to run. In this case, the protocols may reroute.

You cannot configure the router to ignore an Xoff state. FECNs and BECNs take the place of Xoff.

If IP is available, use the Ping trace option to determine which Frame Relay node is down.

Troubleshooting an MCT1 Connection

This section assumes that you have isolated a problem to a multichannel T1 (MCT1) connection. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Appendix A includes instructions on reading MCT1 log messages.

To troubleshoot an MCT1 connection:

1. **Filter the log to display only messages from the MCT1 entity running on the slots experiencing the problem.**

The Technician Interface command is as follows:

```
log -fftwid -eMCT1 -s<slot_no.>
```

Example

If you are filtering events from slots 3 and 4, enter the following command:

```
log -fftwid -eMCT1 -s3 -s4
```



Note: Appendix A includes instructions on reading MCT1 log messages.

2. **Check the following MCT1 MIB entries by entering the following Technician Interface commands:**

```
get wfDrivers.14.0
```

Or, use this Quick Get path: wfSoftwareConfig > wfDrivers > wfMunichLoad.

```
get wfLinkModules.17.0
```

Or, use this Quick Get path: wfSoftwareConfig > wfLinkModules > wfMCT1E1Load.

3. **Make sure that the Line Type and Line Coding supplied by the T1 provider match the associated settings in the MCT1 configuration.**
4. **Make sure that the digital signal, level 0 (DS0) channels match at both the router and the central office.**

5. **Watch the LEDs on the back of the MCT1 module. If the Sync LED keeps flashing, the line build out (LBO) is not in sync. This indicates impedance or resistance on the line. Ask the T1 carrier if you should set it to long haul or short haul, and configure the LBO parameter accordingly.**

The Sync LED stays on when the framer is in sync with the carrier's clock.

6. **Make sure that you set the LBO appropriately.**

For example, 0.0 dB is short haul (up to 133 ft).

7. **Use the MCT1 built-in bit error rate test (BERT) and line loop-up, loop-down, and payload loopbacks for troubleshooting. (This feature is available only with Site Manager in dynamic mode.)**

Note that only one port can be in BERT mode at a time.

Payload loopbacks are available in extended super frame (ESF) line type mode only.

8. **Make sure that the clocking is set to Port1 Ext Loop or Port2 Ext Loop. These settings are equivalent to Sync External.**

The internal clocking of the MCT1 link module is the same as the internal clocking of the T1 link module. The MCT1 Slave and Loop settings are equivalent to the T1 master clock in the T1 link module.

9. **Make sure that the CRC16 (cyclic redundancy check) or CRC32 match the carrier's specifications.**

10. **Make sure that the value of the Inter Frame Time Fill parameter matches idles (0xFF) or flags (0x7E) with the remote end of the link.**

11. **Check the events from the entity DS1E1 (multichannel T1/E1 driver service) to view the MCT1 log events.**

MCT1 uses the wfDS1E1 MIB entries. Therefore, the entity name associated with MCT1 is DS1E1, *not* MCT1.

MCT1 uses the wfSyncEntry object; T1 uses the wfLogicalLineEntry object.

12. **Enter the Technician Interface loadmap <slot_no.> command and make sure that the software loaded the *munich.exe* and *mct1e1.exe* files. If it did not, use the Image Builder to add them to the router software image, and transfer the image to the memory card.**

Troubleshooting a Synchronous Connection

This section assumes that you have isolated a problem to a synchronous connection. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot a synchronous connection as follows:

1. **Filter the log to display only messages from the Sync entity running on the slots experiencing the problem.**

The Technician Interface command is as follows:

log -fftwid -eSYNC -s<slot_no.>

Example

If you are filtering events from slots 3 and 4, enter the following command:

log -fftwid -eSYNC -s3 -s4

If you see a message like the following, see “[Troubleshooting the Internal Clock Settings \(Lab Environments Only\)](#)” later in this chapter:

Warning Sync Code: 40 "Connector COM2: clock speed does not match other ports."

2. **Use the Technician Interface to look at the values of the following attributes in the wfSyncEntry object:**



Note: The **get** command is next to the attribute name. Or, use the Quick Get path wfLine > wfSyncTable.

- wfSyncRuntsRx (**get wfSyncEntry.51.***)

This shows the number of frames received that are smaller than the minimum length. It usually indicates a clocking problem on the line.

- wfSyncBadFramesRx (**get wfSyncEntry.49.***)

This shows the frames received that were unrecognizable. It may indicate underflow errors or an out-of-phase clock on the remote side.

- `wfSyncLackRescRx (get wfSyncEntry.42.*)` and `wfSyncLackRescRx (get wfSyncEntry.43.*)`

This shows the number of times the router dropped frames it received because of a lack of buffers or a lack of space on the transmission queue. Some errors are likely, especially when the router boots. If this number increases to a high rate (such as 15/minute) for an extended period, it may indicate a problem.

Check the `wfKernelEntry` for the slot where the problem is occurring to determine whether buffers are available. To do this, enter the command `get wfKernelEntry.*.<slot>`. For example, enter the following command: `get wfKernelEntry.*.2`. The router reports the number of available buffers in slot 2. If buffers are available, something on the network is preventing the router from updating its buffer lists.

Check for protocol storms (for example, from IP RIP, IPX RIP, and IPX SAP, and learning bridge reconverging). If no buffers are available, check the configuration of the line and the line utilization.

Increase the configured receive queue length (`wfSyncCfgRxQueueLength`) to 64 and see if that alleviates the problem.

- `wfSyncUnderFlowTx (get wfSyncEntry.44.*)`

This shows the number of incomplete frames that the router transmitted because the device queue was empty.

This problem usually occurs when you out-clock the router's port. Certain link modules (such as the DSDE 5430) support only a 600 KB aggregate throughput. If the port is receiving a T1 clock signal, the link will be operational, but underflow errors can occur.

3. Display and record these statistics, wait 1 minute, and repeat the procedure.

Compare the statistics shown each time to determine whether the media is currently experiencing problems. If the error statistics change, check the reception and transmission statistics of the other ports in the same slot.

4. Refer to one of the following sections if it pertains to your problem:

- [“Checking the Address Format \(Bay Networks Standard Only\)”](#)
- [“Troubleshooting a Synchronous to X.21 Connection”](#)
- [“Reception Errors Incrementing or Reception Count Not Incrementing”](#)
- [“Troubleshooting the Internal Clock Settings \(Lab Environments Only\)”](#)

Checking the Address Format (Bay Networks Standard Only)

If the router is running Version 7.0 or later of the Bay Networks Standard PPP, and you defined explicit addressing, make sure the addresses are in decimal format. (The addresses in a Series 5 router are in hexadecimal format.) If the address is greater than 9 and in the wrong format, the synchronous link fails to activate.

Troubleshooting a Synchronous to X.21 Connection

If you connect a Bay Networks router running Series 7 or Series 8 software to a device with an X.21 interface, do the following:

1. **Set the appropriate Com port configuration jumpers on the Ethernet link module to the X.21 setting.**

See Installing and Maintaining BN Routers for instructions.

2. **Enter the following command:**

get wfSyncEntry.76.*

3. **Make sure that you set the synchronous polling in the router's synchronous line driver configuration to 2 (disabled), which is the default.**

If you set synchronous polling to 1 (enabled) and the data set ready (DSR) lead is dropped, the software disables the synchronous driver. When you set it to 2, the software disregards the DSR lead.

Reception Errors Incrementing or Reception Count Not Incrementing

Conduct a local loopback test of the local channel service unit (CSU) or digital service unit (DSU). During the loopback test, check the transmission and reception statistics.



Caution: Do not do loopback testing on a synchronous port during network production time if the bridge is operating on that port.

If transmission and reception statistics increment equally without errors, conduct a loopback test of the remote CSU/DSU if at least one of the following is true:

- You configured the synchronous line as standard with explicit addressing.
- You configured the data terminal equipment/data communications equipment (DTE/DCE) with promiscuous mode turned on.

The remote loopback test allows data to leave the router, cross the synchronous circuit to the remote CSU/DSU, and return to the router.

If the transmission and reception statistics increment without errors, perform the local and remote loopback tests on the remote side.

If the local loopback test did not cause any error count to be incremented, but the remote loopback test did, request that the carrier test the line and remote CSU/DSU.

If the local loopback test causes the error counts to continue to increment, complete one of the following procedures to isolate the problem:

- Disconnect the cable from the port of the router reporting the errors and plug it into another port on the router you know works correctly.

If the synchronous errors persist, verify that you properly configured the newly tested port, test the cable, and test the local CSU/DSU.

If the errors stop, compare the newly tested port's configuration with that of the original port. If the port configurations are the same, try swapping the link module with a new link module.

- Connect the port of the router reporting the errors to another CSU/DSU and monitor the line statistics.

If the errors persist, try another cable or try swapping the link module with a new link module.

Troubleshooting the Internal Clock Settings (Lab Environments Only)

If you are using crossover cables to connect to two back-to-back routers in a lab environment, make sure all interfaces on a given slot have consistent clock source and speed settings. A message such as the following appears if two interfaces on a slot have inconsistent clock settings:

Warning Sync Code: 40 "Connector COM2: clock speed does not match other ports."



Note: All internally clocked ports on a slot change to the last configured internal clock speed when you boot, save a dynamic configuration change, or enter the **config** command.

Check the clock source and speed settings as follows:

1. **Enter the following command to display the clock source setting for each slot and connector in the router:**

get wfSyncEntry.13.*

The display shows the settings for all synchronous ports on all slots in the following format:

```
wfSyncEntry.wfSyncClkSource.<slot_no.>.<connector_no.> =  
<setting>
```

The setting is 1 for internal clocking or 2 for external clocking.

2. **If any of the clock source settings are 1 (for internal clocking), enter the following command to check the clock speed:**

get wfSyncEntry.14.*

The console displays the transmission and reception clock speed for each slot and connector on the router. All ports configured for internal clocking in a slot use the clock speed of the port most recently configured for internal clocking. The clock speed is valid only for the slots that are set for internal clocking.

Valid clock speeds are as follows: 1200 (1200b), 2401 (2400b), 4807 (4800b), 7204 (7200b), 9615 (9600b), 19230 (19200b), 32051 (32000b), 38461 (38400b), 56818 (56k), 64102 (64k), 125000 (125k), 227272 (230k), 416666 (420k), 625000 (625k), 833333 (833k), 1250000 (1mb), 2500000 (2mb), and 5000000 (5mb).

Troubleshooting a Token Ring Connection

This section assumes that you have isolated a problem to a token ring connection. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot a token ring connection as follows:

1. **Filter the log to display only messages from the token ring entity running on the slots experiencing the problem.**

The Technician Interface command is as follows:

log -fftwid -eTOKEN -s<slot_no.>

Example

If you are filtering events from slots 3 and 4, enter the following command:

log -fftwid -eTOKEN -s3 -s4

If token ring Debug Event 36 (Connector MAU<SlotConnector> Ring Status Change<4_digit_hex_code>) appears, convert the 4-digit number from hexadecimal to binary. Assign the position numbers 0 through 10 to the first 11 digits, from left to right.

Look for the position number of the 1 bit in the following list:

- 0 indicates signal loss.
- 1 indicates a hardware error.
- 2 indicates a software error.
- 3 indicates a transmitter beacon.
- 4 indicates a lobe wire fault.
- 5 indicates an automatic removal error.
- 6 is reserved for future use.
- 7 indicates a remove received.
- 8 indicates a counter overflow.
- 9 indicates a single station.
- 10 indicates a ring recovery.

2. If you are using the Technician Interface, enter the following command to list the instances of the wfTokenRingEntry object:

list instances wfTokenRingEntry

3. If you are using the Technician Interface, enter the following command to display the values of the wfTokenRingEntry object for the instance in question:

get wfTokenRingEntry.*.<instance>

Or, use the Quick Get path wfLine > wfTokenRingTable.

4. Look at the values of the following attributes:

- wfTokenRingMadrSelect

This shows the source of the MAC address: boxwide (1), PROM (2), or configuration (3).

- wfTokenRingSpeed

This shows whether the speed is 4 Mb/s (4194304) or 16 Mb/s (16777216).

- wfTokenRingEarlyTokenRelease

This shows whether Early Token Release is enabled (1) or disabled (2). It is valid only when the ring speed is 16 Mb/s.

Troubleshooting Other Data Link Layer Protocols

This section assumes that you have isolated a problem to a data link connection. If not, refer to Chapter 2 to determine if these instructions apply to your problem.

Troubleshoot a data link layer protocol as follows:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for the media in question.**

The Technician Interface command is as follows:

log -fftwid -e<ENTITY> -s<slot_no.>

When specifying <ENTITY>, use uppercase letters. See *Event Messages for Routers* for a list of the entities.

Example

If you are filtering events from the HSSI entity running in slots 3 and 4, enter the following command:

log -fftwid -eHSSI -s3 -s4

2. **Check the state of the media.**
3. **Check the values of the following statistics twice and compare them to determine whether the media is currently receiving/transmitting frames and generating errors:**
 - Reception and transmission statistics

If the reception or transmission statistics do not change, do the following:

 - Check the reception and transmission statistics of the other ports in the same slot.
 - Try disabling and enabling the port, and check the log messages to determine why the connection will not activate.
 - Error statistics
4. **Look at the forwarding tables of each router in the path to determine the following:**
 - Whether entries exist
 - Whether the next-hop addresses are in the right direction

5. **Verify the configuration parameters.**
6. **Use Packet Capture and a network analyzer to check the segments involved in the problem.**

Chapter 6

Troubleshooting a Network Layer Problem

This chapter describes how to solve network layer problems. It assumes that you that have already determined the scope of your problem, as described in Chapter 2.

Topic	Page
Troubleshooting AppleTalk	6-2
Troubleshooting DLSw	6-4
Troubleshooting IP	6-6
Troubleshooting IPX	6-16
Troubleshooting OSI	6-21
Troubleshooting Switched Services	6-23
Troubleshooting Other Network Layer Protocols	6-30

Troubleshooting AppleTalk

This section assumes that you have isolated a problem to AppleTalk. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot AppleTalk problems as follows:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for AppleTalk.**

The Technician Interface command is as follows:

```
log -fftwid -eAT -s<slot_no.>
```

Example

If you are filtering events from slots 3 and 4, enter the following command:

```
log -fftwid -eAT -s3 -s4
```

2. **Enter the following command to check the base records:**

```
get wfAppleBase.*.0
```

The most important attributes are as follows:

- The State attribute shows whether AppleTalk is up (1), down (2), initializing (3), or not present (4). You cannot change this setting.
 - The Disable attribute shows whether AppleTalk is enabled (1) or disabled (2).
3. **Check the values of the following statistics twice and compare them to determine whether AppleTalk is currently receiving/transmitting packets and generating errors:**
 - Reception and transmission statistics

If the reception or transmission statistics do not change, do the following:

 - Check the reception and transmission statistics of the other protocols associated with the same connector and the same slot.
 - Try disabling and enabling AppleTalk, and check the log messages to determine why the connection will not activate.
 - Error statistics
 4. **Make sure that the next hop and network you are trying to reach are in the routing table entries.**

5. **Verify the configuration parameters.**
6. **Use Packet Capture and a network analyzer to check the segments involved in the problem.**

The following sections describe how to respond to certain event messages from AppleTalk:

- [“Local Net Range Conflict Event Message”](#)
- [“Zone . . . Conflict Event Message”](#)
- [“Static Configuration Conflict Event Message”](#)

Local Net Range Conflict Event Message

Configure the router's interface to match the network range configured on the seed router.

The configured network range failed to match that of another seed router's network range. The router sent a request for network information and received a response that contained a network range that was inconsistent with that configured for the interface.

Zone . . . Conflict Event Message

If the message `Zone Name Conflict`, `Number of Zones on Extended Net Conflict`, or `Default Zone-Seed Conflict` appears in the event log, configure the router's interface to match the zones configured on the seed router.

The configured network range failed to match the defined zones of another seed router. The router sent a Zone Information Protocol (ZIP) request and received a response that contained zone information that was inconsistent with that configured for the interface.

The message `Number of Zones on Extended Net Conflict` appears if a zone other than the default zone fails to match that of the seed router, or if the default zone name is in the zone list. The default zone should not be in the zone list.

The message `Default Zone-Seed Conflict` appears if the default zone fails to match that of the seed router.

Static Configuration Conflict Event Message

The node number associated with the interface is already being used by another node on the same segment.

Set the node number of the interface to zero (0) so that it will configure dynamically, or define a unique node ID.

Troubleshooting DLSw

This section assumes that you have isolated a problem to data link switching (DLSw). If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

You can turn on extended DLSw log messages by setting the Max Sessions attribute of the wfDls object to 1111. Bay Networks recommends that you turn off extended DLSw messages when you finish examining the log to test or troubleshoot a DLSw connection.

Troubleshoot a DLSw connection as follows:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for DLSw.**

The Technician Interface command is as follows:

log -fftwid -eDLS -s<slot_no.>

Example

If you are filtering events from slots 3 and 4, enter the following command:

log -fftwid -eDLS -s3 -s4

2. **Make sure that the DLSw MTU size matches the synchronous line MTU size.**

Unnecessary packet fragmentation can occur when these settings do not match.

3. **Use the Technician Interface or the Statistics Manager to inspect the global source route bridge (SRB) settings, such as the internal LAN ID, the group LAN ID, and the bridge ID.**

The Technician Interface command is as follows:

get wfBrSr.*.0

4. **Use the Technician Interface or the Statistics Manager to inspect the global DLSw settings, such as the configured TCP window size and the total number of established DLSw sessions.**

The Technician Interface command is as follows:

get wfDIs.*.0

Make sure that the virtual ring ID for the IP cloud is unique and is consistent among all sites.

5. **Use the Technician Interface or the Statistics Manager to inspect the state of all configured DLSw interfaces, and the value of the instance field.**

The Technician Interface command is as follows:

get wfDIsInterfaceEntry.3.*

6. **Use the Technician Interface or the Statistics Manager to inspect the state of all TCP connections.**

The Technician Interface command is as follows:

get wfTcpConnEntry.2.*

Make sure that all active TCP sessions are in “established” state (represented by the value 5).

If the sessions are in an established state, the local and remote DLSw TCP slot/peer configuration is probably correct.

If the sessions are not in an established state, do the following:

- a. **Make sure all slots configured to run DLSw have an assigned slot IP address.**
- b. **Make sure that the slot IP address corresponds to the DLSw Peers setting at the remote site.**
7. **Use the Technician Interface or the Statistics Manager to inspect the reception messages and connection-state changes.**

Troubleshooting IP

This section assumes that you have isolated a problem to IP. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot an IP connection as follows:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for IP running on the slots in question.**

The Technician Interface command is as follows:

log -fftwid -elP -s<slot_no.>

Example

If you are filtering events from slots 3 and 4, enter the following command:

log -fftwid -elP -s3 -s4

2. **Enter the following command to check the base records:**

get wflpBase.*.0

The most important attributes are as follows:

- The State attribute shows whether IP is up (1), down (2), initializing (3), or not present (4). You cannot change this setting.
- The Create attribute shows whether IP is created (1) or deleted (a number other than 1).
- The Enable attribute shows whether IP is enabled (1) or disabled (2).
- The Forwarding attribute shows whether IP forwards (1) or does not forward (2) datagrams that it received, but that are not addressed.

Example

```
$ get wfIpBase.*.0
wfIpBase.wfIpBaseCreate.0 = 1
wfIpBase.wfIpBaseEnable.0 = 1
wfIpBase.wfIpBaseState.0 = 1
wfIpBase.wfIpBaseForwarding.0 = 1
wfIpBase.wfIpBaseDefaultTTL.0 = 30
wfIpBase.wfIpBaseRipDiameter.0 = 15
wfIpBase.wfIpBaseRouteCache.0 = 60
wfIpBase.wfIpBaseMibTables.0 = 2
wfIpBase.wfIpBaseNetworks.0 = 250
wfIpBase.wfIpBaseZeroSubnetEnable.0 = 2
wfIpBase.wfIpBaseEstimatedNetworks.0 = 0
wfIpBase.wfIpBaseHosts.0 = 81
wfIpBase.wfIpBaseEstimatedHosts.0 = 0
wfIpBase.wfIpBaseDefaultOverSubnetEnable.0 = 2
wfIpBase.wfIpBaseMaxPolicyRules.0 = 32
```

3. Check the values of the following statistics twice in the **wfIpInterfaceEntry** object. Compare them to determine whether IP is currently receiving/transmitting packets and generating errors:

- Reception and transmission statistics

If the reception or transmission statistics do not change, do the following:

- Check the reception and transmission statistics of the other protocols associated with the same connector and the same slot.
- Try disabling and enabling IP, and check the log messages to determine why the connection will not activate.



Caution: Disabling IP disrupts network services.

- Error statistics
4. Make sure that the next hop and network you are trying to reach are in the routing table entries.
 5. Verify the configuration parameters.
 6. Use Packet Capture and a network analyzer to check the segments involved in the problem.

Refer to one of the following sections if it pertains to your problem:

- [“Troubleshooting Telnet, FTP, and TFTP”](#)
- [“Ping Does Not Work”](#)
- [“Troubleshooting RIP”](#)
- [“Troubleshooting OSPF”](#)

Troubleshooting Telnet, FTP, and TFTP

The message `Unknown Network OR Network Unreachable` indicates that the device does not have a path to the requested network.

If the sender and the target are on the same LAN, verify that the network IP address and subnet mask are the same for both interfaces.

If this message appears on a UNIX workstation, issue the **netstat -r** command at the workstation. The command displays the contents of the routing table and any default routes. Check the port's subnet mask, which determines whether networks are local or remote. If the workstation is in routed mode, check the Telnet, FTP, or TFTP daemon configuration.

Troubleshoot a Telnet, FTP, or TFTP connection as follows:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for the application.**

The Technician Interface command is as follows:

```
log -fftwid -e<TELNET | FTP | TFTP>
```

Example

If you are filtering events from Telnet, enter the following command:

```
log -fftwid -eTELNET
```

2. **Enter the following command to check the base records:**

```
get <wfTelnet | wfFtp | wfTftp>.*.0
```

Example

```
get wfTelnet.*.0
```

The Delete attribute appears only in the Telnet and FTP base records. It shows whether the protocol is created (1) or deleted (2).

The Disable attribute shows whether the protocol is enabled (1) or disabled (2).

3. **Ping your interface address.**
4. **Ping the next-hop address listed in the routing table for the network on which the remote host resides.**
5. **Ensure that the ICMP echo outs statistic is increasing for the IP interface.**
6. **Use the ping -p command to trace the path of the ping, look for loops, and determine whether the packet's TTL (time to live) field has timed out.**

The message `Unreachable` indicates that IP does not have a route to the network in the routing table and cannot issue a ping request.

The message `Does not respond` indicates that the router did not receive a response to the ping request.

7. **Check the cabling on the local and remote devices.**
8. **Make sure the application is running on the local and remote devices.**
9. **Make sure the circuit is enabled and activated.**
10. **Make sure the interface is enabled and activated.**
11. **Make sure the next-hop address in the interface routing table is set to:**
 - a. **The address of the interface for any directly connected network**
 - b. **The address of another router's interface on a directly connected network for any non-directly connected network**

Ping Does Not Work



Note: The source address used in any ping (ICMP echo request) originating at the router is always the IP address of the router's outgoing port.

Follow the instructions in the sections that apply:

- [“Router Cannot Ping Another Local Device”](#)
- [“Router Cannot Ping Endstation, Can Ping Other Endstations on the Same Segment”](#)
- [“Endstation Cannot Ping the Remote Interface on the Router”](#)

- [“Endstation Can Ping Devices on the Same Segment, but Cannot Ping the Router”](#)
- [“Endstation Can Ping Local and Remote Interfaces on the Router, but Cannot Ping a Remote Station”](#)

Router Cannot Ping Another Local Device

When the router cannot ping another device on the network, it does not necessarily mean that the network or router is down.

If the device you are trying to ping has never responded successfully to a ping request because it is a new endstation, a new segment, or a new router, make sure that you configured it properly.

If the ping was successful at one time, but is no longer successful, try to isolate the problem to any recent changes in the network. If you do not know of any recent changes, or if you verified that they are OK, do the following:

1. Try to make the endstation ping itself.

If the endstation cannot ping itself, refer to the documentation on the TCP/IP stack and LAN card for that system and inspect the installation and configuration.

An endstation must be able to ping itself in order to receive a ping response from the network. However, the self-ping operation is internal and has nothing to do with the network or the router. Therefore, an improperly configured endstation may be able to ping itself just as easily as a properly configured endstation.

2. Try to make the router ping its own interface.

If the router can ping its own interface, the interface is enabled and the protocols are configured on the port. However, like an endstation, a misconfigured router may be able to ping itself.

If the router cannot ping its own interface, check the log and verify the physical status of the interface.

3. Try to make the endstation ping other interfaces on the same router.

4. Try to make the endstation ping other devices on the same segment.

5. **Enter the Technician Interface `loadmap <slot_no.>` command for each slot and verify that IP and ARP are running on all slots.**
6. **Verify that the ARP cache only has entries for hosts on the local network.**

Refer to the MIB object `wfIpNetToMediaEntry` to locate the ARP cache.

Router Cannot Ping Endstation, Can Ping Other Endstations on the Same Segment

If the router can ping other endstations successfully, but not the endstation in question, and that endstation cannot ping other nodes in the network, do the following:

1. **Verify that the configuration of the endstation is correct.**
2. **Verify that the router's ARP cache contains the endstation's MAC address.**

Refer to the MIB object `wfIpNetToMediaEntry` to locate the ARP cache.

If the MAC address is incorrect, go to the endstation and try to ping the router. The router should update its ARP cache with the correct MAC address. The router's ARP cache entries do not time out unless you enable the HOST/ARP cache.

3. **Look for an entry with alternating MAC addresses.**

If an entry is alternating between one MAC address and another, two devices on the network have the same IP address. Change the IP address of one of the devices.

Endstation Cannot Ping the Remote Interface on the Router

Refer to one of the following sections:

- [“Network Unreachable Message”](#)
- [“Host Did Not Respond Message”](#)

Network Unreachable Message

Verify that the endstation's configuration includes a default gateway.

If an endstation tries to send data to another IP address, it uses its own subnet mask to determine whether the destination is on the same segment (that is, the same network and subnet) or a remote segment (that is, a different network and/or subnet).

If the destination address is on a remote segment, and the endstation's configuration includes a default gateway, it tries to route the packet via the gateway. If the endstation's configuration does not include a default gateway, it displays a `Network Unreachable` message.

Host Did Not Respond Message

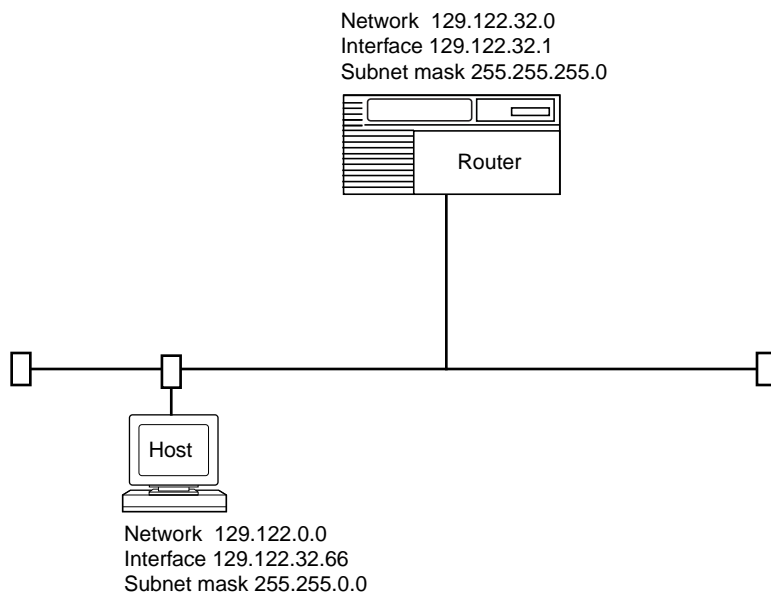
If the endstation or router displays this message, do the following:

1. **Make sure that the endstation configuration includes a default gateway definition or listens to a routing protocol.**
2. **Verify the network addresses of the source and destination devices.**
3. **If the node that did not respond is on a remote segment, verify that each router is correctly resolving the ARP address of the next device in the path.**
4. **If the node that did not respond is on the local segment, use the MIB object `wfIpInterfaceEntry` to verify the address configuration and interface ICMP counters.**

Endstation Can Ping Devices on the Same Segment, but Cannot Ping the Router

If the endstation can ping other devices on the same segment, but cannot ping the local interface of the router, do the following:

1. **Compare the endstation's interface number, network number, and subnet mask to those of the router's interface. The network and subnet numbers must be the same, except that the endstation's subnet mask does not have to include as many octets as the router's subnet mask ([Figure 6-1](#)).**



TRB0006A

Figure 6-1. Comparing the Endstation and Router Configurations

The router uses the subnet mask to determine which traffic to route to each segment. In Figure 6-1, the router's subnet mask must include the third octet if other subnets in the 129.122 network connect to the router. In such configurations, you typically configure Proxy ARP to run on the router's interface because the endstation does not know that it has to go through the router to get to other subnets of the 129.122.0.0 network.

2. **Disable IP on the router's interface, then try to ping the IP address of the router again.**

If the ping succeeds, a device with a duplicate IP address is on the segment.

3. **Enable IP on the router's interface and try to ping other stations on the segment that is reporting problems.**

If the attempts to ping fail, verify that you configured the router with the correct IP network, interface, and subnet addresses.

Endstation Can Ping Local and Remote Interfaces on the Router, but Cannot Ping a Remote Station

If the endstation can ping the local and remote router interfaces but cannot ping a remote station, do the following:

1. **Ping the device on each link in the path between the source and destination to determine the location of the problem.**



Note: Use the Site Manager or Technician Interface **path** option when pinging the remote station. This option provides the same functionality as the UNIX **tracert** command.

2. **Make sure that the next hop for each network points to the correct interface.**
3. **Ping from the remote station to the local station.**

This verifies that each router in the path not only has a route to the remote segment but also has a path back to the originator of the ping request.

Troubleshooting RIP

If the router cannot reach a network or host, determine whether there is an entry for the network or host in the routing table. If the entry is in the routing table, determine whether the next hop and metric are correct.

If the entry is not in the routing table, do the following:

1. **Determine whether the router enabled RIP.**
2. **Set RIP Listen on the RIP interface.**
3. **Determine whether a RIP station on an attached network is sending RIP packets.**
4. **Use Packet Capture or a network analyzer to capture the RIP packets and verify the accuracy of the advertisements from other RIP stations.**

Troubleshooting OSPF

To troubleshoot an OSPF routing problem, do the following:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for OSPF running on the slots in question.**

The Technician Interface command is as follows:

```
log -fftwid -eOSPF -s<slot_no.>
```



Note: In Versions 8.01 and later, you can restrict the amount of OSPF information that appears in a log. Remove these filters when trying to troubleshoot a problem.

Example

If you are filtering events from slots 3 and 4, enter the following command:

```
log -fftwid -eOSPF -s3 -s4
```

2. **Enter the following command to check the base records:**

```
get wfOspfBase.*.0
```

The most important attributes are as follows:

- The State attribute shows whether OSPF is up (1), down (2), initializing (3), or not present (4). You cannot change this setting.
- The Create attribute shows whether OSPF is created (1) or deleted (a number other than 1).
- The Enable attribute shows whether OSPF is enabled (1) or disabled (2).

3. **Check the OSPF neighbor states to compare the exchange state with other OSPF routers on the network.**

Neighbor states should be either two-way or full; the other states (init, exchange start, and loading) are interim (or transition) states. Investigate any routers or links that do not recover from these states.

4. **Look at the link state database (LSDB) of the router.**

This is the information from which the router builds its routing table.

5. **Enter the following command to display the IP forwarding table:**

```
get wflpBaseRtEntry.7.*
```

The Technician Interface displays the table in the following format:

```
wfIpBaseRtEntry.wfIpBaseRouteNextHop.<network> = <next_hop>
```

Identify the incorrect routes. If you take a snapshot of your network periodically (as described in Chapter 1), comparing the data can help you to identify the incorrect routes.

Use Packet Capture or a network analyzer to trace routes through the network to see what, if any, nodes are forwarding incorrect routing information in the form of RIP or link state packets (LSPs).

- 6. Determine whether the link is operational and the communication is bidirectional. You can do this by displaying the MIB object wfOspfIfEntry.**

The display shows the state of OSPF on the interface, the identity of the designated router (DR) and backup designated router (BDR) on the segment, how many hello packets the interface received and transmitted, and how many link state updates it received, and received and transmitted.

Troubleshooting IPX

This section assumes that you have isolated a problem to IPX. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

This section assumes that you have loaded the scripts. See *Using Technician Interface Scripts* for instructions.

Troubleshoot an IPX connection as follows:

- 1. Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for IPX running on the slots in question.**

The Technician Interface command is as follows:

```
log -fftwid -elPX -s<slot_no.>
```

Example

If you are filtering events from slots 3 and 4, enter the following commands:

```
log -fftwid -elPX -s3 -s4
```

2. Make sure that the IPX routing software is activated.

To do this, use the Statistics Manager Quick Get tool to display the value of wfApplication > wfIpxGroup > wfIpxBaseState. Or, use the Technician Interface to load the scripts and enter the following Technician Interface script command:

show ipx base

Example

```
$show ipx base
IPX Base Record Configuration Information
-----
Protocol   State      Router Name
-----
IPX        Up         1

Primary NN   Router Name
-----
None        None

Route Method Mult Host Mode   Maximum Path
-----
Tick Based   Enabled          1

Log Filter Setting          PreConfigured Net Table Size
-----
Filter Trace                0
```

3. Make sure that each configured network is in the up state, and that the network address, host address, and encapsulation method are correct for each circuit.

To do this, use the Statistics Manager to view the IPX Main Information Table screen, or enter the following Technician Interface script command:

show ipx circuit

Example

```
$show ipx circuit
```

```
IPX Circuit Configuration Information (ALL)
```

```
-----
```

Circuit	State	Net Address	Host Address	Encaps Method
-----	-----	-----	-----	-----
O22	Up	0x2E000011	0x0000A20E08D4	LSAP
E44	Up	0x2E008000	0x0000A2030079	Ethernet
E32	Up	0x2E009000	0x0000A2035A5E	LSAP
E33	Up	0x2E010000	0x0000A2035A5F	LSAP
E42	Up	0x2E036000	0x0000A2030077	Novell/802.3
O21	Up	0x2E060010	0x0000A20E08D3	LSAP
O23	Up	0x2E060100	0x0000A20E08D5	LSAP

```
7 Circuits in table.
```



Note: If an interface running IPX and Bridge receives a packet with an IPX encapsulation type that is different from that configured on the interface, the Bridge sends it to other interfaces running Bridge. IPX reads only the IPX packet encapsulation types that you configure it to read. Therefore, you must be careful when configuring the packet encapsulation types in an IPX network.

4. If you configured the router to run RIP, make sure that IPX RIP is up on the circuits in question.

To do this, use the Statistics Manager to view the IPX RIP Interface Table screen, or enter the following Technician Interface script command:

show ipx rip

The IPX RIP Interface Table shows whether you configured the RIP interfaces with RIP Supply, RIP Listen, or Standard (both RIP Supply and RIP Listen).

Example

```
show ipx rip
```

```
IPX RIP Interface Record Configuration Information (All)
```

```
-----
```

RIP Interface	State	Mode
-----	-----	-----
0x2E000011	Up	Standard
0x2E008000	Up	Standard
0x2E009000	Up	Standard
0x2E010000	Up	Standard
0x2E036000	Up	Standard
0x2E060010	Up	Standard
0x2E060100	Up	Standard

5. **Make sure the networks you are trying to reach are in the IPX routing table.**

To do this, use the Statistics Manager to view the IPX Base Route Table screen, or enter the following Technician Interface script command:

show ipx routes

Example

```
$show ipx routes
```

```
IPX Routing Table Information
```

```
-----
```

Destination	NextHop Net	NextHop Host	Method	Age	Ticks	Hops
-----	-----	-----	-----	---	----	---
0x00000002	0x2E060100	0x0000454B2F59	RIP	20	21	12
0x00000003	0x2E060100	0x0000454B2F59	RIP	20	23	13
0x00000022	0x2E060010	0x000045B0F556	RIP	10	15	5
0x00000023	0x2E060010	0x000045B0F556	RIP	10	16	6
0x00000024	0x2E060100	0x0000454B2F59	RIP	20	15	5
0x00000025	0x2E060100	0x0000454B2F59	RIP	20	15	5
0x00000042	0x2E060100	0x0000454B2F59	RIP	30	18	8

Alternatively, you can display a route to a specific destination by entering the following Technician Interface script command:

show ipx route find <destination_address>

Example

```
$show ipx route find 0x00000986
IPX Routing Table Information
```

```
-----
Destination  NextHop Net NextHop Host    Method Age Ticks Hops
-----
0x00000986   0x2E000011  0x0000C9108A7A  RIP   20   2    1
```

6. **Examine the entries in the routing table to make sure that the path to the destination in question is appropriate.**
7. **Make sure that the server you are trying to reach is in the IPX SAP table.**

To do this, use the Statistics Manager to view the IPX Base SAP Table screen, or enter the following Technician Interface script command:

show ipx services

Example

```
$show ipx services
IPX Service Table Information
```

```
-----
Server                                     Service  Age  Hops
Type
-----
QDS                                       0x0004   20   7
EUCLID                                  0x0004   60   8
SYDNEY                                  0x0004   60   7
CALERN                                  0x0004   20   8
CD_ROM                                  0x0004   20   9
NYC1                                    0x0004   60   8
```

8. **To test the service's connectivity to the router, enter the following Technician Interface script command:**

show ipx ping <service_name>

Example

```
$show ipx ping NW312_LOTUS
```

```
IPX Ping command, by name
```

```
-----
Searching for NW312_LOTUS in server database.
Server NW312_LOTUS found, sending ping...
pinging NW312_LOTUS at 0x00000986.0x000000000001
IPX ping: 0x00000986.0x000000000001 is alive
```


Troubleshooting OSI

This section assumes that you have isolated a problem to OSI. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot an OSI connection as follows:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for OSI running on the slots in question.**

The Technician Interface command is as follows:

log -fftwid -eOSI -s<slot_no.>

Example

If you are filtering events from slots 3 and 4, enter the following command:

log -fftwid -eOSI -s3 -s4

2. **Enter the following command to request data from the OSI interface:**

osidata -s<slot no.> -t<type> -i<ID>

<slot no.> is the number of a slot on which the OSI service is running on the router. Valid values are 1 to 13, inclusive.

<type> is the database information you want to display. Valid values are as follows:

- lsp_L1 -- link state packet for level 1
- lsp_L2 -- link state packet for level 2
- path_L1 -- internal path control block for level 1 path
- path_L2 -- internal path control block for level 2 path
- adj_L1 -- adjacency control block for level 1
- adj_L2 -- adjacency control block for level 2
- adj_ES -- adjacency control block for end system

<ID> is the identifier for the database information. The ID varies in length, depending on the type. For example, the lsp ID is 8 bytes, the adj ID is 6 bytes, and the path ID (also referred to as the router ID) is 6 bytes. All identifiers are in hexadecimal notation.

This command allows you to display OSI database information for a particular slot in the router. The display includes information about link state packets (LSPs), path control blocks, and adjacency control blocks.

The console displays the database information you requested or an error message.

For example, if you enter the command **osidata -s 2 -t lsp_L1 -i aaaaaaaaaaaaa0000** to request a level 1 LSP with the LSP ID aaaaaaaaaaaaa0000 from the OSI service installed on slot 2, and the OSI service responds to the request, the Technician Interface console displays messages similar to the following:

```
L2 LSPID aaaaaaaaaaaaa0000
SRM_flags 0 0 0 0, SSN_flags 0 0 0 0, Ctrl flags 8
Lifetime 1200, Seqnum 2, Chksum 9b9a, Flags 03
01040349 0040020c 00148080 80aaaaaa aaaaaa01 0300080 8080aaaa
aaaaaaaa
```

If the OSI service cannot respond to the request for data, the console may display one of the following error messages:

- Invalid slot number, can't parse cmd line
The slot does not exist.
- Invalid ID, can't parse cmd line
You entered a number of bytes other than eight for the LSP ID.
- No answer from called slot
The OSI service is not installed on the specified slot.
- No data returned for ID message
An LSP does not exist for the specified ID on the specified slot.
- Unknown database object type, can't parse cmd line
You entered an invalid value with the **-t<type>** option.

3. To display the LSP ID, use the **osil1lsp** or **osil2lsp** alias, depending on the level (1 or 2).

The alias definitions are as follows:

- **osil1lsp** = echo "L1 LSPDB"; get wfOsiL1LspHdrEntry.1
- **osil2lsp** = echo "L2 LSPDB"; get wfOsiL2LspHdrEntry.1

4. To display the dynamic adjacency ID, use the `osiadjs` alias.

The alias definition is as follows:

```
osiadjs = echo "Dynamic Adjacencies"; get wfOsiDynAdjEntry.9
```

5. To display the path or router ID, use the `osil1routes` or `osil2routes` alias, depending on the level (1 or 2).

The alias definitions are as follows:

- `osil1routes` = echo "L1 Fwd Routes"; get wfOsiL1RouteEntry.1
- `osil2routes` = echo "L2 Fwd Routes"; get wfOsiL2RouteEntry.1

Troubleshooting Switched Services

This section assumes that you have isolated a problem to the switched services. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot switched services as follows:

1. Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for the modem interface and PPP entities running on the slots in question.

The Technician Interface command is as follows:

```
log -fftwid -eMODEMIF -ePPP -s<slot_no.>
```

Example

If you are filtering events from slots 3 and 4, enter the following command:

```
log -fftwid -eMODEMIF -ePPP -s3 -s4
```

2. Inspect the log as follows:

- a. **If the connection is V.25bis, make sure that the modem sent the call request number (CRN).**
- b. **Make sure the telephone number is correct.**

If the modem sent the CRN, the telephone number is correct, and the modem did not dial, check the cabling and configuration of the modem.

c. Determine how PPP is negotiating during the connection.

During a successful connection, the control protocol on both sides of the configured demand circuit comes up and the associated events appear in the log.

3. Filter the log to display messages of all severity levels for the switched services running on the slots in question.

The Technician Interface command is as follows:

log -fttwid -eSWSERV -s<slot_no.>

Example

If you are filtering events from slots 3 and 4, enter the following command:

log -fttwid -eSWSERV -s3 -s4

4. Determine whether the circuit is in slave mode or master mode.

5. Filter the log to display the network layer protocol event messages and determine whether they are activating.

6. Use the Technician Interface get command or the Statistics Manager Quick Get tool to examine the following MIB objects for configuration settings and errors:

```
-- wfPppCircuitEntry
-- wfPppLineEntry
-- wfPPPWhoamiEntry
-- wfSwservOptsEntry
-- wfSwservOutPhoneNumEntry
-- wfModemIfEntry
```

7. If you are running IP with RIP or OSPF for dial backup, do the following:

a. Ping across the connection from the primary line.

If the ping fails and the router fails to establish a backup connection, issue the Technician Interface **show ip arp** script command. Determine whether you statically configured the ARP cache. If you are running Frame Relay on the primary line, configure an IP adjacent host.

- b. **Check the slave site's routing table for the routes it learned from the master site. Do the same when the backup line activates.**

Refer to one of the following sections if it applies to your problem:

- [“Master Cannot Connect to Slave”](#)
- [“Troubleshooting RS-232 Raise DTR Dial Services”](#)
- [“Troubleshooting V.35 Raise DTR Dial \(Balanced\)”](#)
- [“Troubleshooting ISDN BRI and PRI”](#)

Master Cannot Connect to Slave

In a dial-backup application, if the master side cannot connect to the slave side, do the following:

1. **Make sure the configuration file is correct.**
2. **If the connection is V.25bis, check the log for the CRN.**
3. **Try reversing the master and slave.**
4. **Make sure that you enabled BofL on the primary line.**

If you can establish this connection, recheck the configuration of the modem and router.

Troubleshooting RS-232 Raise DTR Dial Services

If a data terminal ready (DTR) signal is activated on the backup circuit (the master side), causing the backup modem to dial even though the primary line is up, do the following:

1. **Verify that the modem is sending a data set ready (DSR) signal to the router interface in the on state (positive voltage) when the local and remote modems are not connected.**

If it is, configure the modem so that DSR follows carrier detect (CD), or configure DSR to be in the off state until the modem receives a DTR signal. Unfortunately, DCE manufacturers use inconsistent terminology for these settings.

When the router detects that DSR is in the on state (positive voltage), it brings DTR high regardless of the state of the primary line. This causes the modem to dial. If the router does not detect any DSR (negative voltage), the router brings DTR high, which causes the modem to dial.

2. **If the router's connection to the modem is a 44-pin synchronous interface, and the modem is a master, make sure the modem can send the ring indicator (RI) signal from Pin 22 to the router interface in the control off state (negative voltage).**

Most RS-232 modems support this control signal. If the modem does not support this control signal, use the Configuration Manager to edit the connector of the backup line, click on Modem, and disable RI.

The RS-232 pin assignments are as follows:

- RI: Pin 22
- DCD: Pin 8
- DTR: Pin 20
- DSR: Pin 6

Troubleshooting V.35 Raise DTR Dial (Balanced)

If the DTR is up when it should not be, causing the modem or CSU to initiate a dial sequence, do the following:

1. **If the router's connection to the modem or CSU is a 44-pin synchronous interface, and the modem is a master, make sure the modem or CSU can send the RI signal from Pin J to the router interface in the control off state.**

Some CSUs do not support the Pin J, RI signal. If the modem or CSU does not support this control signal, use the Configuration Manager to edit the connector of the backup line, click on Modem, and disable RI.

If the CSU does not supply RI Pin J, you can create a custom cable to use another signal, such as RLSD (received line signal detection) Pin F, as RI Pin J. RLSD is typically low until the modem establishes a connection, and goes low again after DTR toggles.



Note: Disabling RI on the router has no effect in this case. The absence of the RI control signal at the master side causes DTR to go high.

2. **Disconnect the local and remote CSUs from the DCE, and use a breakout box to verify whether the DCE (modem or CSU) is sending a DSR signal to the router interface in the on state (positive voltage).**

If it is, configure the DCE for DSR to follow CD, or configure DSR to be in the off state until the DCE receives a DTR signal, and reconnect the CSUs. Unfortunately, DCE manufacturers use inconsistent terminology for these settings.



Note: This is the preferred way to resolve this problem. However, if the CSUs do not support this solution, use the Configuration Manager to edit the connector of the backup line, click on Modem, and disable RI. DTR then goes high only if the primary line becomes unavailable.

The V.35 pin assignments are as follows:

- RLSD (received line signal detection) Pin F
- RI (ring indicator) Pin J
- DSR (data set ready) Pin E
- DTR (data terminal ready) Pin H

Troubleshooting ISDN BRI and PRI

Troubleshoot ISDN BRI and PRI as follows:

1. **For ISDN PRI only, verify that MCT1/MCE1 initialized correctly.**

Example

```
# 7: mm/dd/yy 10:38:39.363  DEBUG  SLOT  4  DS1E1  Code:  50
Connector COM1, Logical Line 1 time_slot = 16.
Connector COM1, Logical Line 1 time_slot = 17.
Connector COM1, Logical Line 1 time_slot = 18.
Connector COM1, Logical Line 1 time_slot = 19.
Connector COM1, Logical Line 1 time_slot = 20.
Connector COM1, Logical Line 1 time_slot = 21.
Connector COM1, Logical Line 1 time_slot = 22.
Connector COM1, Logical Line 1 time_slot = 23.
Connector COM1, Logical Line 1 time_slot = 24.
Connector COM1, Logical Line 1 initialization complete
```

2. **Filter the log to display messages of all severity levels for the ISDN PRI, ISDN BRI, and switched services running on the slots in question.**

The Technician Interface command is as follows:

log -fttwid -eISDN -eISDN_BRI -eSWSERV -s<slot_no.>

Example

If you are filtering events from slots 3 and 4, enter the following command:

log -fttwid -eISDN -eISDN_BRI -eSWSERV -s3 -s4

3. Refer to the log to verify the following:

- Layer 2 and layer 3 of ISDN started.

Example

```
# 21: mm/dd/yy 03:16:08.283 TRACE SLOT 1 ISDN Code: 16
Starting Layer 3.
# 22: mm/dd/yy 03:16:08.286 TRACE SLOT 1 ISDN Code: 13
Starting Layer 2.
```

- The Line Manager initialized.

Example

```
# 3: mm/dd/yy 03:15:49.393 INFO SLOT 1 SWSERV Code: 65
Line Manager Initializing.
```

- The BRI digital subscriber loops (DSLs) are active.

Example

```
# 2: mm/dd/yy 03:15:42.755 INFO SLOT 1 ISDN_BRI Code: 8
ISDN BRI2, DSL 0, Interface enabled.
```

- ISDN assigned the terminal endpoint identifiers (TEIs).

Example

```
# 31: mm/dd/yy 03:16:10.541 INFO SLOT 1 ISDN Code: 4
TEI 64 assigned on DSL 0.
```

- ISDN BRI in North America only: The switched service (SWSERV) entity registered one or more Service Profile Identifiers (SPIDs).

Example

```
# 30: mm/dd/yy 03:16:10.439 INFO SLOT 1 SWSERV Code: 102
Sending Registration for SPID1:4002 on DSL 0.
```

- The ISDN configuration includes the correct switch type.

Example

```
# 11: mm/dd/yy 03:15:49.517 INFO SLOT 1 SWSERV Code: 136
ISDN Configured for switch type BRI Nil.
```

4. Look at the attribute values of the following MIB objects:

- wfIsdnSwitchCfgEntry
- wfPppCircuitEntry
- wfSwservOptsEntry
- wfPppLineEntry
- wfIsdnBriInterfaceEntry
- wfPppWhoamiEntry
- wfSwservOutPhoneNumEntry
- wfIsdnLocalPhoneNumEntry
- wfIsdnPoolEntry
- wfIsdnCallInfoEntry

If a call fails, do the following:

1. **Verify that a line in a pool is available to make a call.**
2. **Verify that a call setup is in the log and that the calling and called numbers are correct.**
3. **If the ISDN connection is present, filter the PPP event messages to verify that the PPP negotiation succeeded.**

The Technician Interface command is as follows:

log -fftwid -ePPP

4. **Verify that the CHAP or PAP data in wfSwservOptsEntry matches that of the remote router's wfPppWhoamiEntry.**

For CHAP, make sure that the secret is identical on both sides of the link.

5. **Verify that the protocol network numbers and adjacent host information are correct.**
6. **If using call screening on incoming calls, verify that the numbers in Dialup > Incoming Phone Numbers match those in the Call Setup messages received.**

Troubleshooting Other Network Layer Protocols

This section assumes that you have isolated a problem to a network layer protocol. If not, refer to Chapter 2 to determine whether these instructions apply to your problem.

Troubleshoot other network layer protocols as follows:

1. **Use the Events Manager or the Technician Interface to filter the log to display messages of all severity levels for the protocol in question.**

The Technician Interface command is as follows:

log -fftwid -e<ENTITY> -s<slot_no.>

When specifying <ENTITY>, use uppercase letters. See *Event Messages for Routers* for a list of the entities.

Example

If you are filtering events from the XNS, entity running in slots 3 and 4, enter the following command:

log -fftwid -eXNS -s3 -s4

2. **Check the base records.**

For example, if you are having a problem with XNS, enter **get wfXnsBase.*.0** to check the status of the software.

The most important attributes are as follows:

- The State attribute shows whether the protocol is up (1), down (2), initializing (3), or not present (4). You cannot change this setting.
- The Create or Delete attribute shows whether the network software is created (1) or deleted (2).
- The Enable or Disable attribute shows whether the protocol is enabled (1) or disabled (2).

3. Check the values of the following statistics twice and compare them to determine whether the protocol is currently receiving/transmitting packets and generating errors:

- Reception and transmission statistics

If the reception or transmission statistics do not change, do the following:

- Check the reception and transmission statistics of the other protocols associated with the same connector and the same slot.
- Try disabling and enabling the protocol, and check the log messages to determine why the connection will not activate.

- Error statistics

4. Make sure that the next hop and network you are trying to reach are in the routing table entries.

5. Verify the configuration parameters.

6. Use Packet Capture and a network analyzer to check the segments involved in the problem.

Chapter 7

Troubleshooting a Site Manager Problem

This chapter describes how to solve Site Manager problems.

Topic	Page
Site Manager Won't Start	7-1
Cannot Establish a Site Manager Session with the Router	7-5
Cannot Allocate Colormap Message	7-9
UNIX Workstation Generating Core Dumps	7-9

Site Manager Won't Start

The following sections describe how to troubleshoot a Site Manager installation:

- [“Site Manager Won't Start on a PC”](#)
- [“Site Manager Won't Start on a UNIX Workstation”](#)

Site Manager Won't Start on a PC

Refer to the section that applies to your problem:

- [“Cannot Find File Message”](#)
- [“Working Directory or Path Is Invalid Message”](#)
- [“Unable to Find UDP Port Numbers for SNMP Message”](#)

Cannot Find File Message

If a message like the one in [Figure 7-1](#) states that the application cannot find the WFSM.EXE or WINSOCK.DLL files when you click on the PC Site Manager icon, install, configure, and test the TCP/IP communication stack.

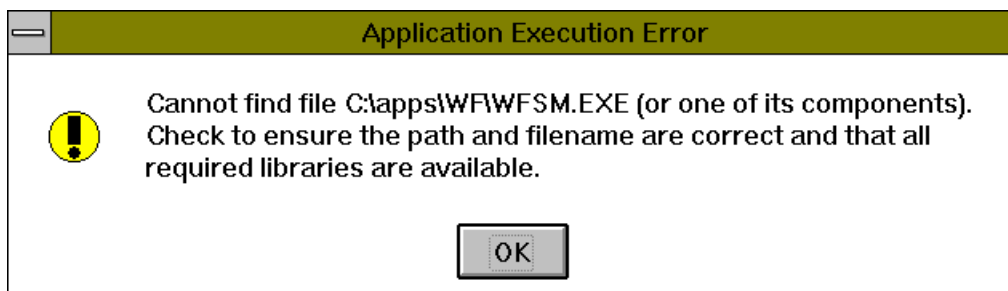


Figure 7-1. Cannot Find File Error Message



Note: You must install a TCP/IP stack such as Chameleon or Distinct TCP/IP and configure it properly before you install Site Manager.

Test the TCP/IP stack as follows:

1. **Use the TCP/IP stack on the PC to ping the interface on the PC's network interface card (NIC).**
2. **Use the TCP/IP stack on the PC to ping another node on the local network.**

If you do not receive a response to the ping request, do the following:

- a. **Check the cable connection to the PC.**
- b. **Check the cable connection to the local node you are trying to ping.**
- c. **Make sure that you configured the TCP/IP stack.**

If you cannot ping a device that can ping other devices, and the cabling is OK, the configuration of the TCP/IP stack is incorrect.

3. **Make sure that the environment variable `PATH` contains only the path to the protocol stack that you want Site Manager to use.**

Otherwise, the PC will boot, but Site Manager may use the wrong protocol stack. It uses the first winsocket library it finds when searching the directories in the environment variable `PATH`.

Working Directory or Path Is Invalid Message

These messages appear when the properties of the PC Site Manager icon fail to match the installation and configuration. Do the following:

1. **Click on the PC Site Manager icon.**
2. **Choose File > Properties.**
The Program Item Properties window opens.
3. **Make sure the settings in the Command Line and Working Directory fields match the directory of the *WFSM.EXE* and configuration files.**

Unable to Find UDP Port Numbers for SNMP Message

The *SERVICES* file is located in:

- The *NETMANAG* directory if you are using Chameleon
- The *ETC* directory if you are using Distinct TCP/IP

Make sure the *SERVICES* file contains the following lines:

```
snmp_trap      162/udp
snmp           161/udp
```

Site Manager Won't Start on a UNIX Workstation

If you are having problems starting Site Manager on a UNIX workstation, do the following:

1. **Verify that the workstation meets all of the minimum system requirements.**
2. **Enter the `wfchkenv` command to verify that the path variables and environment variables are set up correctly.**

Make sure the link `/usr/wf` points to the directory where you installed Site Manager.

3. **Enter the `wfchkinst` command to verify the installation.**
4. **Verify that you updated the `/etc/services` file correctly:**
 - If the workstation running Site Manager is accessing network information services (NIS), update the `/etc/services` file on the workstation that is providing NIS.
 - If the workstation running Site Manager is not accessing NIS, update the `/etc/services` file on the Site Manager workstation.
5. **Verify that no two processes bind to the same SNMP trap port number.**

For example, Site Manager and Sun Net Manager cannot both bind to the SNMP trap port.
6. **Refer to one of the following sections if it applies to your problem:**
 - [“Unable to Load SNMP MIB or File Was Inaccessible Message”](#)
 - [“Unable to Run . . . Module Message”](#)

Unable to Load SNMP MIB or File Was Inaccessible Message

If messages like the following appear, add swap space to your workstation:

```
wfsm: unable to load the SNMP MIB (c3202)
wfsm: The SNMP MIB could not be loaded from the file
/usr/wf/lib/WFMIB.defs
Either the file was inaccessible, or not enough memory to load file
```

Unable to Run . . . Module Message

Before starting Site Manager, make sure that you have write access for the current working directory. If you start Site Manager in a directory where you do not have write access, you will not be able to use the Site Manager tools. A message such as Unable to Run Configuration Module appears.

Cannot Establish a Site Manager Session with the Router

If you cannot establish a connection from Site Manager to a managed router, do the following:

1. **Make sure the IP address in the Router Connections window matches the IP address of the router.**
2. **Increase the timeout and retries settings, then try again.**
3. **Make sure that the IP address of the Site Manager workstation is in the list of the router's community managers.**

You can do this by using another Site Manager workstation or the Technician Interface. Refer to one of the following sections:

- [“Using an Alternative Site Manager Workstation to Enable Access”](#)
- [“Using the Technician Interface to Enable Access”](#)
- [“Cannot Connect Site Manager Running on a PC”](#)
- [“Cannot Connect Site Manager Running on a UNIX Workstation”](#)
- [“Target Does Not Respond \(or Similar Message\)”](#)

Using an Alternative Site Manager Workstation to Enable Access

To enable SNMP access, complete the following procedure using a workstation that allows you to connect to the router:

Site Manager Procedure	
You do this	System responds
1. In the Site Manager main window, choose Tools .	The Tools menu opens.
2. Choose Configuration Manager .	The Configuration Manager menu opens.
3. Choose Dynamic .	The Configuration Manager displays the real-time router hardware and software configuration.
4. Choose Protocols .	The Protocols menu opens.
5. Choose IP .	The IP menu opens.
6. Choose SNMP .	The SNMP menu opens.

Site Manager Procedure <i>(continued)</i>	
You do this	System responds
7. Choose Communities .	The SNMP Community list opens.
8. Choose Community .	The Community menu opens.
9. Choose Managers .	The Manager list opens.
10. If the list does not contain the IP address of the Site Manager workstation that failed, choose Manager.	The Manager menu opens.
11. Choose Add Manager .	The IP address of the Site Manager workstation is added to the Manager list.

Using the Technician Interface to Enable Access

Enable SNMP access as follows:

1. Enter the following Technician Interface command:

get wfSnmpMgrEntry.4.*

The following line appears for each workstation configured as an SNMP manager:

```
wfSnmpMgrEntry.wfSnmpMgrName.<community index>.<IP address> =  
(nil)
```

An IP address of 0.0.0.0 allows any workstation to become an SNMP manager.

2. If the display does not contain the IP address of the Site Manager workstation that failed, assign one.
3. Try again to establish an IP connection with the router.

Cannot Connect Site Manager Running on a PC

Troubleshoot Site Manager connectivity problems on a PC as follows:

1. Ping the local router interface.

If you cannot ping the router, Site Manager cannot communicate with it.

If the ping attempts fail, and the number of transmitted requests and reply counters fail to increment, the PC did not receive a response to the ARP request for the router's MAC address. Do the following:

- a. **Check the configured address of the PC, the subnet mask, and the gateway.**
- b. **Ping other stations on the LAN.**
- c. **Try to ping the router port from other PCs or workstations on the LAN.**

If the ping attempts fail, but the number of transmitted requests increments, the PC has a path to the requested address, but failed to receive a response. Do the following:

- a. **Verify that the router interface has a path to the PC.**
 - b. **Verify that the segment on which the PC is located does not contain duplicate IP addresses.**
 - c. **Issue the Technician Interface `get wflplInterfaceEntry.45.*` command to display the number of ICMP echo requests the interface received for that IP address.**
2. **Once the PC is able to ping the local router interface and receive a response, ping another interface on the router to determine whether the LAN end node knows how to access nodes outside the local network.**
 3. **If the PC cannot ping a remote interface, check the subnet mask and default gateway definitions.**

Cannot Connect Site Manager Running on a UNIX Workstation

Troubleshoot Site Manager connectivity problems on a UNIX workstation as follows:

1. **Log in to an account from which you can run Site Manager.**
2. **Use the command-line interface of the workstation to ping the local router interface.**

If this fails, and the number of transmitted requests and reply counters fail to increment, the workstation did not receive a response to the ARP request for the router's MAC address. Do the following:

- a. **Check the configured address of the workstation and its subnet mask.**
- b. **Try to use the command-line interface to ping other stations on the LAN.**
- c. **Try to ping the router interface from other PCs or workstations on the LAN.**

If the ping attempts fail, but the number of transmitted requests increments, the workstation has a path to the requested address, but failed to receive a response. Do the following:

- a. **Verify that the router interface has a path to the PC.**
 - b. **Verify that the segment on which the workstation is located does not contain duplicate IP addresses.**
 - c. **Issue the Technician Interface `get wflpInterfaceEntry.45.*` to display the number of ICMP echo requests the interface received for that IP address.**
3. **Once the workstation is able to ping the local router interface and receive a response, ping another interface on the router to determine whether the LAN end node knows how to access nodes outside the local network.**
 4. **If the workstation cannot ping a remote interface, check the routing table.**

Target Does Not Respond (or Similar Message)

When the destination of the ping request fails to respond, determine whether the node is in the local ARP cache by issuing the **arp -a** command. Most UNIX workstations display the current ARP cache in response to this command. If the MAC address is in the ARP cache, check its `wfIpInterfaceEntry` statistics.

If the MAC address is not in the ARP cache, do the following:

1. **Enter the following command to check the workstation's interface definition:**

ifconfig -a

The workstation displays all of the assigned IP addresses and subnet masks.

2. **From other nodes on the segment, ping the router's interface.**
3. **From other nodes on the segment, ping the workstation from which you are trying to establish a Site Manager connection.**

Cannot Allocate Colormap Message

Site Manager cannot allocate any colors for its display because another process on the workstation is using them. Set the background to a single color or terminate another background process.

UNIX Workstation Generating Core Dumps

Divide one core dump into smaller files as follows:

1. **Enter the following Technician Interface command:**

gdb -c core

The Technician Interface displays the path and name of the file that was executing.

2. **Enter the command again, this time using the path and name of the executable file displayed in step 1 as a variable:**

gdb -c core <pathname>

3. **Send the files to the Bay Networks Technical Solutions Center.**

See Chapter 8 for instructions.

Chapter 8

Getting Help

This chapter explains how to get help from Bay Networks when you are unable to resolve a problem using the documentation.

Topic	Page
Reporting a Problem to the Bay Networks Technical Solutions Center	8-1
Sending and Retrieving Files	8-3



Note: The procedures in this chapter assume that you have a Bay Networks service contract. For information about or to purchase a service contract, see “Bay Networks Customer Service” on page xxiii.

Reporting a Problem to the Bay Networks Technical Solutions Center

This section identifies the information Bay Networks needs when you call to report a problem. For the telephone and fax numbers of the Bay Networks Technical Solutions Centers, see “How to Get Help” on page xxiii.

Before you call, prepare to answer the following questions to help expedite a solution to your problem:

1. What is the site ID?

This number allows Bay Networks to track your problem and look up related problems for the site. It also allows Bay Networks to do a case history of the router(s) in question.

2. What is the service contract type?

3. What is the router's serial number?

Enter the Technician Interface command **get wfHwBase.3.0** to display the serial number. Or, use the Quick Get tool to display wfHardwareConfig > wfHwBase > wfHwBpSerialNumber.

4. What are the symptoms of the problem?

5. What workaround are you using?

6. When did the problem start occurring?

7. Under what conditions does the problem occur?

8. What, if anything, has changed in the router and/or network?

9. Can you reproduce the problem, and if so, how?

10. How is the problem affecting your network?

11. What revision of software is currently installed?

12. Does the log show you any additional information?

13. Do you have a trace of the problem?

14. Can you send the Bay Networks Technical Solutions Center a copy of the configuration file and a binary version of the log file?

Go to the next section for instructions.

15. Can Bay Networks dial in to the router using Telnet and troubleshoot the problem?

16. If Bay Networks does not have an up-to-date diagram of your network, can you fax it?

Sending and Retrieving Files

Sending your configuration files, traces, and router event logs can help Bay Networks to isolate and solve the problem with your router. You can send files to and receive them from Bay Networks by using one of the following methods:

- Use the Bay Networks anonymous FTP file server.
- If you can access the Internet, you can use FTP to send configuration files, traces, router event logs, and so on.
- Use an asynchronous file transfer program such as Procom.
- Connect a modem to the problem router and Bay Networks will use XMODEM commands to retrieve configuration files, logs, and traces.
- Fax copies to the Bay Networks Technical Solutions Center.



Note: Although Bay Networks has a bulletin board available to contracted support customers, you cannot transfer files over it.

Use the Bay Networks anonymous FTP file server as follows:

1. **Enter the following command:**
ftp 192.32.253.5
2. **Enter the following after the Name prompt:**
anonymous
3. **Enter the following after the Password prompt:**
ident
4. **To send a file, enter `cd incoming`; to retrieve a file, enter `cd outgoing`.**
5. **If your company does not have a dedicated directory, enter the following command to create one:**
`mkdir <your_company_directory_name>`
6. **Enter the following command to access your company directory:**
`cd <your_company_directory_name>`

7. Enter the following command to specify a binary transmission:
bin
8. Enter **put <filename>** if you are sending a file; enter **get <filename>** if you are retrieving a file.
9. When a message indicates that the binary transmission was successful, enter the **quit** command to exit the FTP session.

Appendix A

Reading the Event Log

This appendix provides examples and explanations of the descriptive text in event messages and debug messages.

Topic	Page
System Startup	A-2
Dial-on-Demand Raise DTR Log	A-18
Dial-on-Demand V.25bis	A-23
MCT1 Log Information in a Lab Environment	A-29

See *Configuring ATM Services* for sample ATM events.



Note: For readability, this appendix does not show redundant messages or those that do not pertain to the topic.

This appendix does not identify the components of an event. See *Event Messages for Routers* for this information.

System Startup

The following sample message is from a log of a Series 7 router after it was restarted with the **boot 2:- 2:log.cfg** command. This message indicates that the system is preparing the router software image.

```
@ 29: mm/dd/yy 11:48:14.507  DEBUG # 2          BOOT ( 12)  Image is in
compressed format... decompressing
```

The boot PROM generates the following message for each slot. This message shows the revision of the boot PROM on the FRE processor module, *not* the revision of software.

```
@ 12: mm/dd/yy 11:47:57.007  INFO # 3          GAME ( 11) Starting image
rel<revision_no.>/boot Day MMM DD 00:12:43 EDT yyyy
```

Because the router received instructions to perform a named boot (that is, a boot with a specified router software image or configuration file on slot 2), the system does *not* query the backplane for the router software image. Slot 2 becomes the server of the router software image. The router bootstraps the loader software and loads the router software image (in this example, *bn.exe*) from the memory card in slot 2.

```
@ 25: mm/dd/yy 11:48:06.058  DEBUG # 3          GAME ( 66)  BackBone(s)
became (re)connected
+ starting Loader
+ LOADER: starting gate 0x0000e @ 0x3050ced2 (env=0x00000000,
flags=0x00000001)
@ 26: mm/dd/yy 11:48:08.054  DEBUG # 2          GAME ( 66)  BackBone(s)
became (re)connected
+ starting Loader
+ LOADER: starting gate 0x0000e @ 0x3050ced2 (env=0x00000000,
flags=0x00000001)
@ 27: mm/dd/yy 11:48:12.695  DEBUG # 2          NVFS ( 37)  Memory Card
Inserted: FLASH (EMBEDDED ALGORITHMS) Memory Type Detected
+ Flash media info: Mfg ID 0x1, Device ID 0x29, number of chips 8
@ 28: mm/dd/yy 11:48:12.695  DEBUG # 2          BOOT (  6)  Found image
'bn.exe' on local file system... booting
@ 29: mm/dd/yy 11:48:14.507  DEBUG # 2          BOOT ( 12)  Image is in
compressed format... decompressing
```

FSM (finite state machine) messages indicate slot-to-slot communication. Each slot is in one of four states: DOWN, SYNC, ACTIV (active), and HOLD.

Each slot transmits BofL requests via the backplane to the other slots in the router in order to determine which slots are active. Each slot transmits 16 BofL requests per second. The operating system logs the status of each slot as follows:

- If a slot does not hear from a remote slot within 4 seconds (64 BofL requests), it logs the state of that slot as **DOWN**.
- If a slot receives some BofL responses from a remote slot, or does not receive all that it should have, it logs the state of that slot as **SYNC**.
- If a slot receives all of the necessary BofL responses from a remote slot that it previously determined as **DOWN** or **SYNC**, it logs a message stating that the remote slot is “reconnected” to the backplane.

For example, in message 40, slot 3 declares that slot 2 is back up.

```
@ 30: mm/dd/yy 11:48:19.153 DEBUG # 3      GAME (74) @REMOTE2 FSM:
FLOW -> HOLD (00014a: TIME-OUT -- last=0000f6)
@ 31: mm/dd/yy 11:48:19.153 WARN # 3      GAME ( 8) slot 2 became
disconnected
@ 32: mm/dd/yy 11:48:21.273 DEBUG # 2      GAME ( 73) @REMOTE 3
FSM: FLOW -> ACTIV (0000f9: 90000007 00012d 20000000 00000000)
+ @REMOTE 3 FSM: ACTIV -> DOWN (0000f9: 90000007 00014d 00000000
20000000)
@ 33: mm/dd/yy 11:48:21.273 WARN # 2      GAME ( 8) slot 3 became
disconnected
@ 34: mm/dd/yy 11:48:21.343 DEBUG # 2      GAME ( 73) @REMOTE 3
FSM: DOWN -> SYNC (0000fa: 90000007 000171 00000000 00000000)
@ 35: mm/dd/yy 11:48:21.386 DEBUG # 2      GAME ( 73) @REMOTE 3
FSM: SYNC -> ACTIV (0000fb: 90000006 000172 20000000 20000000)
@ 36: mm/dd/yy 11:48:21.386 INFO # 2      GAME (10) slot 3 became
re-connected
@ 37: mm/dd/yy 11:48:21.602 DEBUG # 3      GAME ( 73) @REMOTE 2
FSM: HOLD -> DOWN (000171: a0000007 0000f9 00000000 00000000)
@ 38: mm/dd/yy 11:48:21.658 DEBUG # 3      GAME ( 73) @REMOTE 2
FSM: DOWN -> SYNC (000171: a0000006 0000fa 10000000 10000000)
@ 39: mm/dd/yy 11:48:21.860 DEBUG # 3      GAME ( 73) @REMOTE 2
FSM: SYNC -> ACTIV (000175: a0000007 0000fd 10000000 10000000)
@ 40: mm/dd/yy 11:48:21.860 INFO # 3      GAME (10) slot 2 became
re-connected
```

The router is loading the router software image.

```
@ 41: mm/dd/yy 11:48:22.269 DEBUG # 2      BOOT (13) Image loaded,
jumping to: 0x30024000
@ 42: mm/dd/yy 11:48:26.007 INFO # 2      GAME (11) Starting image
rel/9.00 Fri Jul 28 17:12:26 EST 1995
```

The software running in slot 2 synchronized the system clock (WCLK) with the other slots in the router.

```
@ 43: mm/dd/yy 11:48:25.265  DEBUG # 2          GAME (124)  WCLK set:
new=b1506bc9.84a00000 old=b1506bc9.44000000 rtc=b1506bca.00000000
```

```
+ WCLK set: err=00000000.00000000 cor=00000000.00000000
inc=00000000.00000000
```

Slot 2 is attempting to read the *log.cfg* configuration file specified in the boot command from the memory card in slot 2. The NVFS (non-volatile file system) entity is responsible for reading and writing to the memory card.

```
@ 57: mm/dd/yy 11:48:34.314  DEBUG # 2          GAME ( 66)  BackBone(s)
became (re)connected
+ starting Loader
@ 58: mm/dd/yy 11:48:34.318  DEBUG # 2          LOADER (  2)  Loader
starting service gate 0x000a1 @ 0x300a22ea (env=0x00004009, flags=0x1)
@ 59: mm/dd/yy 11:48:34.322  DEBUG # 2          GAME (200)  Board ID
Client: slot 2, type 2
@ 60: mm/dd/yy 11:48:34.439  DEBUG # 2          LOADER (  2)  Loader
starting service gate 0x00066 @ 0x30041692 (env=0x00004009, flags=0x1)
@ 61: mm/dd/yy 11:48:34.459  DEBUG # 2          NVFS ( 60)  Memory card
inserted: FLASH (EMBEDDED ALGORITHMS) memory type detected
+ Memory card media info: Mfg ID 0x1, Device ID 0x29, number of chips 8
@ 62: mm/dd/yy 11:48:34.459  INFO  # 2          NVFS ( 42)  Service
initializing.
@ 63: mm/dd/yy 11:48:34.564  DEBUG # 2          LOADER (  2)  Loader
starting service gate 0x00013 @ 0x30095442 (env=0x00004009, flags=0x1)
@ 64: mm/dd/yy 11:48:34.564  DEBUG # 2          MIB ( 12)  Attempting to
obtain config file
@ 65: mm/dd/yy 11:48:34.564  DEBUG # 2          GAME ( 84)  FWD [ 2-0007]
(a0000013->90000011): down=10000000, no_ACK=00000000, NAK=10000000
```

Slot 2 received a boot request from slot 3.

```
@ 66: mm/dd/yy 11:48:34.658  DEBUG # 2          BOOT (  3)  Boot service
request received from 0x1000000e
```

Slot 2 is reporting that messages it sent to slot 3 were not acknowledged. Slot 3 is unable to respond because it is still booting.

The software interface to the kernel provides for the transmission of both unreliable and reliable messages. The two types of reliable messages are GFWD (GAME forward) and GRPC (GAME remote procedure call). An example of a GFWD message failure logged by slot 2 follows.

```
@ 67: mm/dd/yy 11:48:34.701 DEBUG # 2      GAME ( 84) FWD [ 2-0008]
(a0000013->90000011): down=10000000, no_ACK=00000000, NAK=10000000
@ 68: mm/dd/yy 11:48:34.822 DEBUG # 2      GAME ( 84) FWD [ 2-0009]
(a0000013->90000011): down=10000000, no_ACK=00000000, NAK=10000000
@ 69: mm/dd/yy 11:48:34.955 DEBUG # 2      GAME ( 84) FWD [ 2-000a]
(a0000013->90000011): down=10000000, no_ACK=00000000, NAK=10000000
```

Slot 2 reads the configuration file *log.cfg*.

```
@ 70: mm/dd/yy 11:48:35.150 INFO # 2      MIB ( 4) Using
configuration file '2:log.cfg'
@ 71: mm/dd/yy 11:48:35.221 DEBUG # 2      NVFS ( 63) NVFS manager
is opening file 'log.cfg' for reading
@ 72: mm/dd/yy 11:48:35.271 DEBUG # 2      NVFS ( 64) NVFS manager
is closing file 'log.cfg'
@ 73: mm/dd/yy 11:48:35.279 DEBUG # 2      MIB ( 66) Initializing
MIB with configuration file information
@ 74: mm/dd/yy 11:48:35.354 INFO # 2      MIB ( 3) Service
initializing.
@ 75: mm/dd/yy 11:48:35.377 DEBUG # 2      MIB ( 70) Config manager
loading a 7.60 type configuration.
```

A soloist is a software entity that runs on only one slot in the router at a time. The Technician Interface and TI_RUI (the remote command-line interpreter) soloists are starting up and determining which slot to run on (the election process). The gate ID for the Technician Interface is 0x15. The gate ID for TI_RUI is 0x57.

```
@ 76: mm/dd/yy 11:48:35.393 DEBUG # 2      LOADER ( 2) Loader
starting service gate 0x0000c @ 0x3003a926 (env=0x00000000, flags=0x1)
@ 77: mm/dd/yy 11:48:35.393 DEBUG # 2      GAME ( 23) SOLO
(0x00015): election opening 30000000/30000000 (30000000) vote=00000000
@ 78: mm/dd/yy 11:48:35.424 DEBUG # 2      MIB ( 61) D/A: Loaded
13 MIB mappings.
@ 79: mm/dd/yy 11:48:35.506 DEBUG # 2      GAME ( 97) SOLO
(0x00015): election WON 0x20000000 (repl=b0000009/30000000)
@ 80: mm/dd/yy 11:48:35.510 DEBUG # 2      GAME ( 23) SOLO
(0x00015): election CLOSING 30000000/30000000 (30000000) vote=00000000
@ 81: mm/dd/yy 11:48:35.533 DEBUG # 2      LOADER ( 2) Loader
starting service gate 0x0001e @ 0x300a1fa2 (env=0x00000000, flags=0x1)
@ 82: mm/dd/yy 11:48:35.541 INFO # 2      NOV_SYNC ( 2) Service
initializing.
@ 83: mm/dd/yy 11:48:35.584 DEBUG # 2      GAME ( 97) SOLO
(0x00015): election CLOSED 0x20000000 (repl=b0000009/30000000)
@ 84: mm/dd/yy 11:48:35.662 DEBUG # 2      LOADER ( 2) Loader
starting service gate 0x04016 @ 0x30039a2e (env=0x00000000, flags=0x1)
@ 85: mm/dd/yy 11:48:35.732 DEBUG # 2      BOOT ( 3) Boot service
request received from 0x1000000e
```

```
@ 86: mm/dd/yy 11:48:35.740 DEBUG # 2      GAME ( 23) SOLO
(0x00057): election opening 30000000/30000000 (30000000) vote=00000000
@ 87: mm/dd/yy 11:48:35.783 DEBUG # 2      LOADER ( 2) Loader
starting service gate 0x00050 @ 0x30058392 (env=0x00000000, flags=0x1)
@ 88: mm/dd/yy 11:48:35.877 DEBUG # 2      GAME ( 97) SOLO
(0x00057): election WON 0x20000000 (repl=b0000009/30000000)
+ SOLO (0x00057): election CLOSING 30000000/30000000 (30000000)
vote=00000000
@ 93: mm/dd/yy 11:48:35.967 DEBUG # 2      GAME ( 97) SOLO
(0x00057): election CLOSED 0x20000000 (repl=b0000009/30000000)
```

Learning Bridge (LB) is initializing.

```
@ 94: mm/dd/yy 11:48:35.971 INFO # 2      LB ( 2) Service
initializing.
@ 95: mm/dd/yy 11:48:36.006 DEBUG # 2      LB ( 63) CCT 811521904
update gate initializing.
```

Slot 3 is loading the router software image from slot 2.

```
@ 97: mm/dd/yy 11:48:36.050 DEBUG #3      BOOT (21) Server on slot
2 chosen for BB boot transaction
@ 104: mm/dd/yy 11:48:36.104 DEBUG # 3      BOOT ( 18) BB boot
transaction started:
+ start address 0x30024000, size 0x000c89e0, checksum 0x038D2F95
@ 105: mm/dd/yy 11:48:36.179 DEBUG # 3      BOOT ( 17) Client is
dropping duplicate reply from server 0x2000000D
+ - server seq 0, client seq 4780
```

The statistic and alarm soloist (gate ID 0x95) and the file system control soloist (gate ID 0x98) are electing slots to run on.

```
@ 107: mm/dd/yy 11:48:36.346 DEBUG # 2      GAME ( 23) SOLO
(0x00095): election OPENING 30000000/30000000 (30000000) vote=00000000
@ 108: mm/dd/yy 11:48:36.361 DEBUG # 2      GAME ( 97) SOLO
(0x00095): election WON 0x20000000 (repl=b0000009/30000000)
+ SOLO (0x00095): election CLOSING 30000000/30000000 (30000000)
vote=00000000
@ 109: mm/dd/yy 11:48:36.361 INFO # 2      STA ( 5) Service
initializing.
@ 110: mm/dd/yy 11:48:36.385 DEBUG # 2      GAME ( 97) SOLO
(0x00095): election CLOSED 0x20000000 (repl=b0000009/30000000)
@ 111: mm/dd/yy 11:48:36.385 DEBUG # 2      LOADER ( 2) Loader
starting service gate 0x00095 @ 0x300a0932 (env=0x00000000, flags=0x3)
@ 112: mm/dd/yy 11:48:36.502 DEBUG # 2      LOADER ( 2) Loader
starting service gate 0x00074 @ 0x300a17b2 (env=0x00000000, flags=0x1)
@ 113: mm/dd/yy 11:48:36.502 INFO # 2      SYS ( 3) Service
initializing.
@ 114: mm/dd/yy 11:48:36.510 WARN # 2      SYS ( 2) No system
record configured, creating one.
```



```
@ 115: mm/dd/yy 11:48:36.631  DEBUG # 2      GAME ( 23) SOLO
(0x00098): election opening 30000000/30000000 (30000000) vote=00000000
@ 116: mm/dd/yy 11:48:36.643  DEBUG # 2      GAME ( 97) SOLO
(0x00098): election WON 0x20000000 (repl=b0000009/30000000)
@ 117: mm/dd/yy 11:48:36.646  DEBUG # 2      GAME ( 23) SOLO
(0x00098): election CLOSING 30000000/30000000 (30000000) vote=00000000
@ 118: mm/dd/yy 11:48:36.658  DEBUG # 2      GAME ( 97) SOLO
(0x00098): election CLOSED 0x20000000 (repl=b0000009/30000000)
```

Each slot loads only the configured board drivers and protocols. It queries the router software image and loads the necessary code onto the requesting FRE processor module.

```
@ 122: mm/dd/yy 11:48:37.178  DEBUG # 2      NVFS ( 63) NVFS manager
is opening file 'bn.exe' for reading
@ 123: mm/dd/yy 11:48:37.217  DEBUG # 2      LOADER ( 30) Image
qenet.exe loaded successfully from 2:bn.exe
@ 124: mm/dd/yy 11:48:37.217  DEBUG # 2      NVFS ( 64) NVFS manager
is closing file 'bn.exe'
@ 125: mm/dd/yy 11:48:37.225  DEBUG # 2      LOADER ( 15) Loader
starting application qenet.exe, address 0x30541a10, gate id = 0x00045
@ 127: mm/dd/yy 11:48:37.252  INFO # 2      MODULE ( 7) Service
initializing.
+ QENET I/O module is present.
```

IP loaded successfully and is initializing. IP indicates that it is in “router” mode, rather than “host only” mode (message 133).

```
@ 128: mm/dd/yy 11:48:38.018  DEBUG # 2      LOADER ( 30) Image ip.exe
loaded successfully from 2:bn.exe
@ 129: mm/dd/yy 11:48:38.018  DEBUG # 2      NVFS ( 64) NVFS manager
is closing file 'bn.exe'
@ 130: mm/dd/yy 11:48:38.049  DEBUG # 2      LOADER ( 15) Loader
starting application ip.exe, address 0x304e9770, gate id = 0x00048
@ 132: mm/dd/yy 11:48:38.080  INFO # 2      IP ( 4) Protocol
initializing
@ 133: mm/dd/yy 11:48:38.092  DEBUG # 2      IP ( 8) IP Redirector
Mode: Router
```

Slot 3 successfully loaded the router software image from slot 2 and is starting up.

```
@ 134: mm/dd/yy 11:48:38.259  DEBUG # 3      BOOT ( 19) BB boot
transaction completed!! Jumping to address 0x30024000
```

DECnet loaded successfully onto slot 2 and is initializing.

```
@ 135: mm/dd/yy 11:48:38.631  DEBUG # 2      LOADER ( 30) Image drs.exe
loaded successfully from 2:bn.exe
```

```
@ 137: mm/dd/yy 11:48:38.646 DEBUG # 2      LOADER ( 15) Loader
starting application drs.exe, address 0x304d4eb0, gate id = 0x00054
@ 139: mm/dd/yy 11:48:38.697 INFO # 2      DECnet ( 2) Protocol
initializing.
```

The IP RTM (routing table manager) is setting a bit map to indicate which slots it is running on. Convert the hexadecimal number to binary format; then, read the bit string from left to right. The leftmost bit is always 1. The second leftmost bit is for slot 1, the third for slot 2, the fourth for slot 3, and so on. A map change occurs whenever the IP RTM starts up or terminates on another slot.

```
@ 140: mm/dd/yy 11:48:38.885 DEBUG # 2      IP ( 8) RTM self map
old 49, new a0000049
```

IPX loaded successfully onto slot 2 and the router software image was closed. The operating system opens and closes the router software image whenever it needs to read an executable component.

```
@ 141: mm/dd/yy 11:48:39.428 DEBUG # 2      LOADER ( 30) Image ipx.exe
loaded successfully from 2:bn.exe
@ 142: mm/dd/yy 11:48:39.428 DEBUG # 2      NVFS ( 64) NVFS manager
is closing file 'bn.exe'
```

IPX initialized and the IPX RTM and IPX STM (server table manager) are starting up and setting the maps to indicate which slots they are running on. The configured IPX network number is 000000aa.

```
@ 143: mm/dd/yy 11:48:39.447 DEBUG # 2      LOADER ( 15) Loader
starting application ipx.exe, address 0x304afec0, gate id = 0x0006b
@ 144: mm/dd/yy 11:48:39.471 DEBUG # 2      IPX ( 28) IPX RTM up on
slot 2.
@ 145: mm/dd/yy 11:48:39.471 INFO # 2      IPX ( 1) IPX Protocol
initializing.
@ 146: mm/dd/yy 11:48:39.479 DEBUG # 2      IPX ( 38) IPX STM up on
slot 2.
@ 147: mm/dd/yy 11:48:39.486 DEBUG # 2      IPX ( 41) IPX STM self
map old 0000006E, new A000006E.
@ 149: mm/dd/yy 11:48:39.518 DEBUG # 2      IPX ( 25) IPX DARP gate
for slot 2 is up.
@ 150: mm/dd/yy 11:48:39.525 DEBUG # 2      IPX ( 40) IPX RTM self
map old 0000006C, new A000006C.
@ 151: mm/dd/yy 11:48:39.545 DEBUG # 2      NVFS ( 63) NVFS manager
is opening file 'bn.exe' for reading
@ 152: mm/dd/yy 11:48:39.564 INFO # 2      IPX ( 42) IPX ADD Nwif
cct 1 Network 00.00.00.aa
@ 153: mm/dd/yy 11:48:39.568 INFO # 2      IPX ( 43) IPX Nwif from
MIB Active cct 1 Network 00.00.00.aa
+ IPX Network 00.00.00.aa mapped to cct 1
```

SNMP loaded successfully from the router software image and the SNMP gate soloist SNMP_START elects a slot to run on.

```
@ 154: mm/dd/yy 11:48:39.752 DEBUG # 2      LOADER ( 30) Image
snmp.exe loaded successfully from 2:bn.exe
@ 155: mm/dd/yy 11:48:39.756 DEBUG # 2      NVFS ( 64) NVFS manager
is closing file 'bn.exe'
@ 156: mm/dd/yy 11:48:39.764 DEBUG # 2      LOADER ( 15) Loader
starting application snmp.exe, address 0x304a86e0, gate id = 0x00019
@ 157: mm/dd/yy 11:48:39.768 INFO # 2      SNMP ( 7) Protocol
initializing.
@ 158: mm/dd/yy 11:48:39.791 DEBUG # 2      SNMP ( 36) Agent received
new community public, assigned index 1.
@ 159: mm/dd/yy 11:48:39.811 DEBUG # 2      SNMP ( 38) Agent received
new manager 0 for community index 1
@ 161: mm/dd/yy 11:48:39.861 DEBUG # 2      SNMP ( 40) Agent spawned
the Trap Manager.
@ 162: mm/dd/yy 11:48:39.869 DEBUG # 2      GAME ( 23) SOLO
(0x0001b): election opening 30000000/30000000 (30000000) vote=00000000
@ 163: mm/dd/yy 11:48:39.869 DEBUG # 2      SNMP ( 24) Trap Manager
initializing.
```

The driver for the Ethernet controller chip set (ILACC) loads onto slot 2 and initializes.

```
@ 164: mm/dd/yy 11:48:39.943 DEBUG # 2      LOADER ( 30) Image
ilacc.exe loaded successfully from 2:bn.exe
@ 165: mm/dd/yy 11:48:39.943 DEBUG # 2      NVFS ( 64) NVFS manager
is closing file 'bn.exe'
@ 166: mm/dd/yy 11:48:39.951 DEBUG # 2      LOADER ( 15) Loader
starting application ilacc.exe, address 0x304a6100, gate id = 0x00040
@ 167: mm/dd/yy 11:48:39.955 INFO # 2      CSMACD ( 9) Service
initializing.
@ 168: mm/dd/yy 11:48:39.994 INFO # 2      CSMACD ( 11) Connector
XCVR1 enabled.
@ 169: mm/dd/yy 11:48:39.998 DEBUG # 2      CSMACD ( 18) Connector
XCVR1 initialization complete
+ Environment address - 304e1a00
+ Line record address - 305390a4
+ Hardware map address - 305c5ce4
+ Receive descriptor ring - 80000800
+ Transmit descriptor ring - 80000c00
+ Initialization block - 80007000
+ Silicon revision - 5
```

Slot 3 is booting Version 9.00 of *bn.exe*.

```
@ 176: mm/dd/yy 11:48:41.007 INFO # 3      GAME ( 11) Starting image
rel/9.00 Fri Jul 28 17:12:26 EST 1995
```

The transceiver on slot 2, connector 1, does *not* have SQE (signal quality error) enabled. It reports the absence of an SQE signal, even though it does not need it.

```
@ 193: mm/dd/yy 11:48:45.018 WARN # 2 CSMACD ( 7) Connector
XCVR1 no SQE.
```

Data Path elects the circuit control gate for circuit 1. Each circuit must have a circuit control gate.

```
@ 195: mm/dd/yy 11:48:45.025 DEBUG # 2 DP ( 23) Creating
Circuit 1 soloist with line GH 0x4082
@ 196: mm/dd/yy 11:48:45.025 DEBUG # 2 GAME ( 23) SOLO
(0x00401): election opening 30000000/30000000 (30000000) vote=00000000
@ 197: mm/dd/yy 11:48:45.049 DEBUG # 2 GAME ( 97) SOLO
(0x00401): election WON 0x20000000 (repl=b0000009/30000000)
@ 198: mm/dd/yy 11:48:45.053 DEBUG # 2 GAME ( 23) SOLO
(0x00401): election CLOSING 30000000/30000000 (30000000) vote=00000000
```

ARP initializes successfully on circuit 1.

```
@ 199: mm/dd/yy 11:48:45.057 INFO # 2 ARP ( 1) Service is up
on circuit 1
```

Data Path registers the ISAP (internal services access point) for ARP. The protocol type for ARP is 0806; this type determines that the ARP traffic will go to the correct gate and code according to the Data Path. The number preceding the protocol type indicates the packet format (1 = Ethernet type 2, 2 = 802.2, 3 = SNAP [Subnetwork Access Protocol], 4 = Novell, and so on). Data Path registers Ethernet Type II or SNAP ARP frames on circuit 1. In this example, Data Path does not register the 802.2 ARP frame type. If circuit 1 received an 802.2 ARP frame, ARP would not receive it; instead, it would go to the Learning Bridge.

```
@ 201: mm/dd/yy 11:48:45.135 DEBUG # 2 DP ( 34) ISAP 0x30806
registered on cct 1.
@ 202: mm/dd/yy 11:48:45.140 DEBUG # 2 DP ( 34) ISAP 0x10806
registered on cct 1.
@ 205: mm/dd/yy 11:48:45.213 DEBUG # 2 ARP ( 3) Arp Client
128.128.2.2 registered
```

Data Path always registers Ethernet and SNAP frames for IP. In this example, Data Path registers ISAPs on circuit 1 for the following protocols: IP (Ethernet type 0800), IPX (Ethernet type 8137), and DECnet (Ethernet type 6003). The number preceding the protocol indicates the packet format.

Notice how DECnet only registers one packet type, while two IPX packet types are registered. This is because two unique IPX networks, each with a different packet encapsulation type, are on circuit 1.

```
@ 217: mm/dd/yy 11:48:45.494  DEBUG # 2      DP ( 34)  ISAP 0x30800
registered on cct 1.
@ 218: mm/dd/yy 11:48:45.518  DEBUG # 2      DP ( 34)  ISAP 0x10800
registered on cct 1.
@ 219: mm/dd/yy 11:48:45.537  DEBUG # 2      DP ( 34)  ISAP 0x16003
registered on cct 1.
@ 222: mm/dd/yy 11:48:45.592  DEBUG # 2      DP ( 34)  ISAP 0x38137
registered on cct 1.
@ 225: mm/dd/yy 11:48:45.623  DEBUG # 2      DP ( 34)  ISAP 0x18137
registered on cct 1.
```

Slot 3 boots successfully and is attempting to load the configuration file from slot 2.

```
@ 227: mm/dd/yy 11:48:49.521  DEBUG # 3      GAME ( 66)  BackBone(s)
became (re)connected
+ starting Loader
@ 228: mm/dd/yy 11:48:49.525  DEBUG # 3      LOADER ( 2)  Loader
starting service gate 0x000a1 @ 0x300a22ea (env=0x00006009, flags=0x1)
@ 229: mm/dd/yy 11:48:49.529  DEBUG # 3      GAME (200)  Board ID
Client: slot 3, type 2
@ 230: mm/dd/yy 11:48:49.529  DEBUG # 2      GAME (199)  Board ID
Server: slot 3, type 2
@ 231: mm/dd/yy 11:48:49.537  DEBUG # 3      GAME (201)  Board ID
Client reply: slot 2, type 2
@ 232: mm/dd/yy 11:48:49.646  DEBUG # 3      LOADER ( 2)  Loader
starting service gate 0x00066 @ 0x30041692 (env=0x00006009, flags=0x1)
@ 233: mm/dd/yy 11:48:49.771  DEBUG # 3      LOADER ( 2)  Loader
starting service gate 0x00013 @ 0x30095442 (env=0x00006009, flags=0x1)
@ 234: mm/dd/yy 11:48:49.771  DEBUG # 3      MIB ( 12)  Attempting to
obtain config file
@ 235: mm/dd/yy 11:48:49.787  DEBUG # 3      MIB ( 64)  Getting
configuration from slot 2
@ 236: mm/dd/yy 11:48:49.865  DEBUG # 2      MIB ( 15)  Serving
configuration to slot 0x90000013
@ 237: mm/dd/yy 11:48:49.869  DEBUG # 2      MIB ( 16)  Finished
serving configuration to slot 0x90000013
@ 238: mm/dd/yy 11:48:49.932  DEBUG # 3      MIB ( 13)  Received
configuration from remote slot 0xa0000011
@ 239: mm/dd/yy 11:48:49.936  INFO  # 3      MIB ( 3)   Service
initializing.
@ 240: mm/dd/yy 11:48:49.959  DEBUG # 3      MIB ( 70)  Config manager
loading a 7.60 type configuration.
```

Slot 3 tries to start the Technician Interface and TI_RUI soloists, but because they are already running on slot 2, the soloist elections fail (and are logged as LOST).

```
@ 244: mm/dd/yy 11:48:50.045  DEBUG # 3      GAME ( 97) SOLO
(0x00015): election LOST 0xb0000000 (repl=b0000009/30000000)
+ SOLO (0x00015): election CLOSING 30000000/30000000 (30000000)
vote=00000000
@ 245: mm/dd/yy 11:48:50.072  DEBUG # 3      GAME ( 97) SOLO
(0x00015): election CLOSED 0x10000000 (repl=b0000009/30000000)
@ 246: mm/dd/yy 11:48:50.107  DEBUG # 3      GAME ( 23) SOLO
(0x00057): election opening 30000000/30000000 (30000000) vote=00000000
@ 247: mm/dd/yy 11:48:50.115  DEBUG # 3      LOADER ( 2) Loader
starting service gate 0x0001e @ 0x300alfa2 (env=0x00000000, flags=0x1)
@ 248: mm/dd/yy 11:48:50.115  INFO # 3      NOV_SYNC ( 2) Service
initializing.
@ 249: mm/dd/yy 11:48:50.123  DEBUG # 3      GAME ( 97) SOLO
(0x00057): election LOST 0xb0000000 (repl=b0000009/30000000)
+ SOLO (0x00057): election CLOSING 30000000/30000000 (30000000)
vote=00000000
@ 250: mm/dd/yy 11:48:50.131  DEBUG # 3      GAME ( 97) SOLO
(0x00057): election CLOSED
0x10000000 (repl=b0000009/30000000)
```

The configuration file has a different link module than the one actually in the slot.

```
@ 273: mm/dd/yy 11:48:51.240  WARN # 3      LOADER ( 6) Link Module
on slot 3 misconfigured - ignoring
```

Slot 3 uses the dynamic loader to load the necessary executable modules from slot 2's memory, not the memory card in slot 2. However, if a module is not in slot 2's memory, the dynamic loader gets it from the router software image on the memory card.

```
@ 275: mm/dd/yy 11:48:51.275  DEBUG # 2      LOADER ( 32) Loader
serving request for ip.exe from 0x1000602a
+ Loader serving request for snmp.exe from 0x1000602b
@ 276: mm/dd/yy 11:48:51.279  DEBUG # 3      LOADER ( 27) Dynamic
loader transaction with slot 2 server for ip.exe:
+ start address 0x304E9770, size 0x00020984, checksum 0x00976221
@ 277: mm/dd/yy 11:48:51.279  DEBUG # 2      LOADER ( 32) Loader
serving request for tftp.exe from 0x1000602c
@ 278: mm/dd/yy 11:48:51.291  DEBUG # 3      LOADER ( 27) Dynamic
loader transaction with slot 2 server for snmp.exe:
+ start address 0x304A86E0, size 0x00007204, checksum 0x00211745
@ 279: mm/dd/yy 11:48:51.295  DEBUG # 3      LOADER ( 27) Dynamic
loader transaction with slot 2 server for tftp.exe:
+ start address 0x304A2190, size 0x00003f54, checksum 0x00127cd1
@ 280: mm/dd/yy 11:48:51.303  DEBUG # 2      LOADER ( 33) Loader
service completed for tftp.exe, 0x1000602c
@ 281: mm/dd/yy 11:48:51.318  DEBUG # 3      LOADER ( 28) Dynamic
loader completed transaction for tftp.exe
```

```
@ 282: mm/dd/yy 11:48:51.326  DEBUG # 3      LOADER ( 15) Loader
starting application tftp.exe, address 0x304e7f20, gate id = 0x0001c
@ 283: mm/dd/yy 11:48:51.326  DEBUG # 2      LOADER ( 33) Loader
service completed for snmp.exe, 0x1000602b
@ 284: mm/dd/yy 11:48:51.330  INFO  # 3      TFTP (  2) Protocol
initializing.
@ 285: mm/dd/yy 11:48:51.330  DEBUG # 3      TFTP ( 15) Subsystem
transitioned to DOWN state.
@ 286: mm/dd/yy 11:48:51.357  DEBUG # 3      LOADER ( 28) Dynamic
loader completed transaction for snmp.exe
@ 287: mm/dd/yy 11:48:51.365  DEBUG # 3      LOADER ( 15) Loader
starting application snmp.exe, address 0x304ebe90, gate id = 0x00019
@ 288: mm/dd/yy 11:48:51.377  INFO  # 3      SNMP (  7) Protocol
initializing.
@ 289: mm/dd/yy 11:48:51.408  DEBUG # 3      SNMP ( 36) Agent received
new community public, assigned index 1.
@ 290: mm/dd/yy 11:48:51.432  DEBUG # 3      SNMP ( 38) Agent received
new manager 0 for community index 1
@ 291: mm/dd/yy 11:48:51.475  DEBUG # 2      LOADER ( 33) Loader
service completed for ip.exe, 0x1000602a
@ 298: mm/dd/yy 11:48:51.572  DEBUG # 3      LOADER ( 28) Dynamic
loader completed transaction for ip.exe
@ 299: mm/dd/yy 11:48:51.600  DEBUG # 3      LOADER ( 15) Loader
starting application ip.exe, address 0x304f30b0, gate id = 0x00048
```

The IP RTM updates its bit map to indicate it is running on slot 3.

```
@ 300: mm/dd/yy 11:48:51.623  INFO  # 3      IP (  4) Protocol
initializing
@ 301: mm/dd/yy 11:48:51.631  DEBUG # 2      IP (  8) RTM self map
old a0000049, new b0000049
```

Slot 3 reads the driver needed for a SYNC port from *bn.exe*.

```
@ 309: mm/dd/yy 11:48:52.080  DEBUG # 2      NVFS ( 63) NVFS manager
is opening file 'bn.exe' for reading
@ 310: mm/dd/yy 11:48:52.564  DEBUG # 3      LOADER ( 30) Image
hdlc.exe loaded successfully from 2:bn.exe
@ 311: mm/dd/yy 11:48:52.564  DEBUG # 2      NVFS ( 64) NVFS manager
is closing file 'bn.exe'
@ 312: mm/dd/yy 11:48:52.584  DEBUG # 3      LOADER ( 15) Loader
starting application hdlc.exe, address 0x304d2130, gate id = 0x00041
@ 313: mm/dd/yy 11:48:52.588  INFO  # 3      SYNC (  7) Service
initializing.
```

AppleTalk (entity AT) loads successfully and initializes on slot 3. The operating system elects to run the AppleTalk MIB soloist on slot 3, and AppleTalk updates the AT RTM bit map accordingly.

```
@ 314: mm/dd/yy 11:48:52.689 DEBUG # 2      NVFS ( 63) NVFS manager
is opening file 'bn.exe' for reading
@ 316: mm/dd/yy 11:48:53.229 DEBUG # 3      LOADER ( 30) Image at.exe
loaded successfully from 2:bn.exe
@ 321: mm/dd/yy 11:48:53.256 DEBUG # 3      LOADER ( 15) Loader
starting application at.exe, address 0x304bc3c0, gate id = 0x00071
@ 322: mm/dd/yy 11:48:53.260 DEBUG # 2      TFTP ( 16) Subsystem
transitioned to READY state.
+ Client initialized.
@ 323: mm/dd/yy 11:48:53.283 INFO # 3  APPLETALK ( 4) Protocol
initializing
@ 324: mm/dd/yy 11:48:53.369 DEBUG # 3      GAME ( 23) SOLO
(0x000a5): election opening 30000000/30000000 (30000000) vote=00000000
@ 325: mm/dd/yy 11:48:53.381 DEBUG # 3      GAME ( 97) SOLO
(0x000a5): election WON 0x10000000 (repl=b0000009/30000000)
+ SOLO (0x000a5): election CLOSING 30000000/30000000 (30000000)
vote=00000000
@ 326: mm/dd/yy 11:48:53.396 DEBUG # 3      GAME ( 97) SOLO
(0x000a5): election CLOSED 0x10000000 (repl=b0000009/30000000)
@ 327: mm/dd/yy 11:48:53.404 DEBUG # 3  APPLETALK ( 43)
at_rtm_self_map: old 00000072 new 90000072
@ 328: mm/dd/yy 11:48:53.416 DEBUG # 3  APPLETALK ( 43)
at_mib_solo_chg: BECAME_LOCAL old 000000a5 new 900000a5
+ at_rtm_self_chg: old 00000072 new 90000072
```

The following log messages show what happens when you use the Configuration Manager in dynamic mode to create TCP and Telnet. The subsequent lines show that the MIB entity modifies the MIB objects for TCP and Telnet, thereby causing these applications to initialize.

```
@ 343: mm/dd/yy 11:50:29.005 INFO # 2      MIB ( 7) wfSnmp.3.0 set
to 128.128.2.3
@ 344: mm/dd/yy 11:50:29.096 INFO # 2      MIB ( 5) wfTcp.2.0 set
to 1
@ 345: mm/dd/yy 11:50:29.741 INFO # 2      MIB ( 9) wfNode.2.0 set
to 0x51e3200000000000
@ 346: mm/dd/yy 11:50:45.598 INFO # 2      MIB ( 5) wfTelnet.2.0
set to 1
@ 347: mm/dd/yy 11:50:45.839 INFO # 2      MIB ( 9) wfNode.2.0 set
to 0x51e3200400000000
```


The object wfProtocols is the protocol bit-map object. Each attribute is a different protocol. Every time you add or delete a protocol from a slot, the MIB entity updates the bit map for that protocol. Do *not* try to use the Technician Interface to update this field.

```
@ 348: mm/dd/yy 11:50:46.188 INFO # 2 MIB ( 6)
wfProtocols.18.0 set to 1610612736
@ 349: mm/dd/yy 11:50:46.420 INFO # 2 MIB ( 6)
wfProtocols.15.0 set to 1610612736
```

NVFS reads the Telnet and TCP executable modules from the memory card in slot 2; the dynamic loader loads them in slot 2.

```
@ 350: mm/dd/yy 11:50:46.762 DEBUG # 2 NVFS ( 63) NVFS manager
is opening file 'bn.exe' for reading
@ 351: mm/dd/yy 11:50:46.932 DEBUG # 3 LOADER ( 27) Dynamic
loader transaction with slot 2 server for tcp.exe:
+ start address 0x304797B0, size 0x0000cec4, checksum 0x00394408
@ 352: mm/dd/yy 11:50:47.015 DEBUG # 3 LOADER ( 28) Dynamic
loader completed transaction for tcp.exe
@ 353: mm/dd/yy 11:50:47.032 DEBUG # 3 LOADER ( 15) Loader
starting application tcp.exe, address 0x304ad4d0, gate id = 0x0007b
@ 354: mm/dd/yy 11:50:47.061 INFO # 3 TCP ( 5) TCP is UP.
@ 355: mm/dd/yy 11:50:47.086 DEBUG # 2 LOADER ( 30) Image tcp.exe
loaded successfully from 2:bn.exe
@ 356: mm/dd/yy 11:50:47.086 DEBUG # 2 NVFS ( 64) NVFS manager
is closing file 'bn.exe'
@ 357: mm/dd/yy 11:50:47.107 DEBUG # 2 LOADER ( 15) Loader
starting application tcp.exe, address 0x304797b0, gate id = 0x0007b
@ 358: mm/dd/yy 11:50:47.123 DEBUG # 2 LOADER ( 32) Loader
serving request for tcp.exe from 0x10006057
@ 359: mm/dd/yy 11:50:47.139 INFO # 2 TCP ( 5) TCP is UP.
@ 360: mm/dd/yy 11:50:47.180 DEBUG # 2 LOADER ( 33) Loader
service completed for tcp.exe, 0x10006057
@ 361: mm/dd/yy 11:50:47.259 DEBUG # 2 NVFS ( 63) NVFS manager
is opening file 'bn.exe' for reading
@ 362: mm/dd/yy 11:50:47.553 DEBUG # 3 LOADER ( 30) Image tn.exe
loaded successfully from 2:bn.exe
@ 363: mm/dd/yy 11:50:47.569 DEBUG # 3 LOADER ( 15) Loader
starting application tn.exe, address 0x304a3cb0, gate id = 0x00076
+ Loader serving request for tn.exe from 0x200040df
@ 364: mm/dd/yy 11:50:47.569 INFO # 3 TELNET ( 4) Connection
Manager initializing.
@ 365: mm/dd/yy 11:50:47.598 DEBUG # 3 TCP ( 14) TCP Open req:
0.0.0.0,23 - 0.0.0.0,0 TCB: 0x30530670
@ 366: mm/dd/yy 11:50:47.639 DEBUG # 3 LOADER ( 33) Loader
service completed for tn.exe, 0x200040df
```

```

@ 367: mm/dd/yy 11:50:47.660 INFO # 3      TCP ( 6) TCP Opened:
0.0.0.0,23 - 0.0.0.0,0 TCB: 0x30530670
@ 368: mm/dd/yy 11:50:47.660 INFO # 3      TELNET ( 5) Connection
Manager listening on TCP port 23
@ 369: mm/dd/yy 11:50:47.745 DEBUG # 2      NVFS ( 64) NVFS manager
is closing file 'bn.exe'
@ 370: mm/dd/yy 11:50:47.766 DEBUG # 2      LOADER ( 27) Dynamic
loader transaction with slot 3 server for tn.exe:
+ start address 0x304A3CB0, size 0x00009808, checksum 0x002bb03b
@ 371: mm/dd/yy 11:50:47.853 DEBUG # 2      LOADER ( 28) Dynamic
loader completed transaction for tn.exe
@ 372: mm/dd/yy 11:50:47.866 DEBUG # 2      LOADER ( 15) Loader
starting application tn.exe, address 0x3046ff90, gate id = 0x00076
@ 373: mm/dd/yy 11:50:47.866 INFO # 2      TELNET ( 4) Connection
Manager initializing.
@ 374: mm/dd/yy 11:50:47.886 DEBUG # 2      TCP ( 14) TCP Open req:
0.0.0.0,23 - 0.0.0.0,0 TCB: 0x304e6830
@ 375: mm/dd/yy 11:50:47.923 DEBUG # 2      IP ( 36) Client on
128.128.2.2 for TCP local 23 remote 0 is up
@ 376: mm/dd/yy 11:50:47.943 INFO # 2      TCP ( 6) TCP Opened:
0.0.0.0,23 - 0.0.0.0,0 TCB: 0x304e6830
@ 377: mm/dd/yy 11:50:47.943 INFO # 2      TELNET ( 5) Connection
Manager listening on TCP port 23
@ 378: mm/dd/yy 11:50:49.031 DEBUG # 2      IP ( 36) Client on
128.128.2.2 for TCP local 23 remote 0 is up

```

The following log messages show what happens when you remove the link module in slot 3. Data Path kills the gate assigned to the circuit that becomes unavailable.

```

@ 383: mm/dd/yy 11:51:10.612 WARN # 2      MODULE ( 3) I/O module has
been removed.
@ 386: mm/dd/yy 11:51:10.632 DEBUG # 2      DP ( 23) dp_line_map -
Line GH 0xa0004082 died, cct 1
@ 387: mm/dd/yy 11:51:10.640 DEBUG # 2      DP ( 41) LINE_DOWN msg
rcvd for line gate 0x20004082 on cct 1.
+ Found dead line 0x20004082 at offset 0
+ Last line 0x20004082 in cct 1 died, killing circuit gate
+ DP killing CC gate for cct 1.

```

In this example, the user issued a command to save a log file to the memory card.

```

@ 403: mm/dd/yy 11:52:07.684 DEBUG # 2      NVFS ( 63) NVFS manager
is opening file 'log.sav' for writing

```

Dial-on-Demand Raise DTR Log

The following log shows a successful dial-on-demand connection between the COM2 port in slot 2 and a modem configured for Raise DTR.

These messages appear only when you click on the port configured for dial-on-demand, and set the Debug option under the Modem definition to Enabled. If you are using the Technician Interface, set attribute #29 (the debug attribute) of the object wfModemIfEntry to 1 (1 = enabled, 2 = disabled). The Debug option is available with router software Version 8.01 and later.

The following message indicates that the Sync software module enabled the COM2 port:

```
# 33: mm/dd/yy 14:14:02.826 INFO SLOT 2 SYNC Code: 9
Connector COM2 enabled.
```

The port completes initialization.

```
# 34: mm/dd/yy 14:14:03.095 DEBUG SLOT 2 SYNC Code: 16
Connector COM2 initialization complete
Environment address - 3051f040 Line record address - 3052d8bc
Hardware map address - 30514f9c Initialization block -
80007800
Receive descriptor ring - 80005000 Transmit descriptor ring -
80005800
# 35: mm/dd/yy 14:14:03.095 DEBUG SLOT 2 PCAP Code: 67
interface became local - line 202102
intf gate spawned - line 202102
# 36: mm/dd/yy 14:14:03.103 DEBUG SLOT 2 PCAP Code: 65
wait_state - line 202102
```

The FSM messages indicate that the modem and the router are communicating. The first FSM message shows the state the router was in when the FSM Event that follows occurred.

```
# 37: mm/dd/yy 14:14:04.100 DEBUG SLOT 2 SWSERV Code: 46
Connector COM2: FSM State: RDTR_DISCONNECTED(0)
Connector COM2: FSM Event: RDTR_EVENT_CCT_UP(1); isdn flags: 0x0
```

The following messages indicate that you configured the port for Raise DTR, rather than V.25bis, and remind you to check the modem connection:

```
# 38: mm/dd/yy 14:14:04.100 INFO SLOT 2 MODEMIF Code: 22
Connector COM2: enable requested on cct 65535
Connector COM2: Starting, raise dtr mode, is modem connected and turned
on?
```

The following messages appear even if you did not connect a modem to the router. Unlike V.25bis, Raise DTR does not look for a pin signal to detect whether the port is attached to a modem.

```
# 39: mm/dd/yy 14:14:04.104 INFO SLOT 2 MODEMIF Code: 52
Connector COM2: Circuit has been brought up.
# 40: mm/dd/yy 14:14:04.104 DEBUG SLOT 2 SWSERV Code: 46
Line Mgr received line ready for line 2
# 41: mm/dd/yy 14:14:04.104 INFO SLOT 2 SWSERV Code: 10
Sync Line 2 available for dial on demand pool 2.
# 42: mm/dd/yy 14:14:04.108 INFO SLOT 2 SYNC Code: 11
Connector COM2 providing LLC1 service.
# 43: mm/dd/yy 14:14:04.636 DEBUG SLOT 2 SWSERV Code: 46
Connector COM2: FSM State: RDTR_WAIT_DATA_OR_IND(1)
Connector COM2: FSM Event: RDTR_EVENT_CD_UP(6); isdn flags: 0x24
# 44: mm/dd/yy 14:15:07.770 INFO SLOT 2 SWSERV Code: 23
Data received for dial on demand circuit 3.
```

The log messages stop here until you connect and turn on a modem. After you do this, the router raises DTR to signal the local modem to dial the phone number of the remote modem. The router then pings the remote side of the dial-on-demand link, and displays a DATA Available message when it receives a response.

```
# 45: mm/dd/yy 14:15:07.774 DEBUG SLOT 2 SWSERV Code: 46
Connector COM2: FSM State: RDTR_WAIT_DATA_OR_IND(1)
Connector COM2: FSM Event: RDTR_EVENT_DATA_AVAIL(5); isdn flags: 0x2c
# 46: mm/dd/yy 14:15:07.774 TRACE SLOT 2 MODEMIF Code: 34
Connector COM2: DATA Available.
```

The software assigns a valid circuit number to the line.

```
# 47: mm/dd/yy 14:15:07.774 DEBUG SLOT 2 SWSERV Code: 44
SW Sent you are cc 3 message to line 2
# 48: mm/dd/yy 14:15:07.782 INFO SLOT 2 SWSERV Code: 7
Dial on demand circuit being established on line 2.
```

The router waits for DSR to come up to indicate that the modem established a connection to the remote node.

```
# 49: mm/dd/yy 14:15:32.552 DEBUG SLOT 2 SWSERV Code: 46
Connector COM2: FSM State: RDTR_WAIT_FOR_DSR(2)
Connector COM2: FSM Event: RDTR_EVENT_DSR_UP(3); isdn flags: 0x2e
```

DSR is up.

```
# 50: mm/dd/yy 14:15:32.552 TRACE SLOT 2 MODEMIF Code: 54
Connector COM2: DSR has come up.
# 51: mm/dd/yy 14:15:32.552 INFO SLOT 2 MODEMIF Code: 31
Connector COM2: Connection established.
```

The PPP link over the dial-on-demand circuit establishes an LCP (Link Control Protocol) connection. The messages beginning with message 57 show that the IP software starts and establishes a connection over the dial-on-demand link.

```
# 52: mm/dd/yy 14:15:32.552 TRACE SLOT 2 PPP Code: 43
Sending LCP Configure-Request on circuit 3.
# 53: mm/dd/yy 14:15:32.681 TRACE SLOT 2 PPP Code: 55
Received LCP Configure-Ack on circuit 3.
# 54: mm/dd/yy 14:15:34.867 TRACE SLOT 2 PPP Code: 43
Sending LCP Configure-Request on circuit 3.
# 55: mm/dd/yy 14:15:34.875 TRACE SLOT 2 PPP Code: 54
Received LCP Configure-Request on circuit 3.
Sending LCP Configure-Ack on circuit 3.
# 56: mm/dd/yy 14:15:34.992 TRACE SLOT 2 PPP Code: 55
Received LCP Configure-Ack on circuit 3.
# 57: mm/dd/yy 14:15:34.992 INFO SLOT 2 PPP Code: 38
Link Establishment Phase complete on circuit 3.
Starting Network Control Protocols on circuit 3.
# 58: mm/dd/yy 14:15:34.992 TRACE SLOT 2 PPP Code: 43
Sending IPCP Configure-Request on circuit 3.
# 59: mm/dd/yy 14:15:34.996 INFO SLOT 2 PPP Code: 28
LCP up on circuit 3.
# 60: mm/dd/yy 14:15:35.003 TRACE SLOT 2 PPP Code: 54
Received IPCP Configure-Request on circuit 3.
# 61: mm/dd/yy 14:15:35.007 TRACE SLOT 2 PPP Code: 63
IPCP Naking IP-Address option value 0x0 with value 0x3030301 on circuit
3.
Sending IPCP Configure-Nak on circuit 3.
# 66: mm/dd/yy 14:15:35.117 TRACE SLOT 2 PPP Code: 55
Received IPCP Configure-Ack on circuit 3.
# 67: mm/dd/yy 14:15:35.128 TRACE SLOT 2 PPP Code: 54
Received IPCP Configure-Request on circuit 3.
# 68: mm/dd/yy 14:15:35.132 TRACE SLOT 2 PPP Code: 44
Sending IPCP Configure-Ack on circuit 3.
# 69: mm/dd/yy 14:15:35.132 INFO SLOT 2 PPP Code: 28
IPCP up on circuit 3.
```

The following messages indicate that the Raise DTR signal causes the software to establish the link and activate the upper-layer protocol. ULI stands for upper-layer indication:

```
# 70: mm/dd/yy 14:15:35.136 DEBUG SLOT 2 SWSERV Code: 46
Connector COM2: FSM State: RDTR_WAIT_FOR_ULI(3)
Connector COM2: FSM Event: RDTR_EVENT_ULI_IND(8); isdn flags: 0x22e
# 71: mm/dd/yy 14:15:56.980 DEBUG SLOT 2 SWSERV Code 46
Connector COM2: FSM State: RDTR_CONNECTED(4)
Connector COM2: FSM Event: RDTR_EVENT_DSR_DN(4); isdn flags: 0x224
```

The router detected that the modem dropped DSR, indicating that the remote link is lost.

```
# 72: mm/dd/yy 14:15:56.980 TRACE SLOT 2 MODEMIF Code: 32
Connector COM2: DSR lost connection closed.
```

The router exceeds its inactivity timeout threshold, and drops DTR to terminate the connection to the modem.

```
# 73: mm/dd/yy 14:15:56.980 DEBUG SLOT 2 SWSERV Code: 46
isdn_down_cct - calling drop_dtr
```

The router disables PPP.

```
# 74: mm/dd/yy 14:15:56.980 INFO SLOT 2 PPP Code: 31
Stopping Network Control Protocols on circuit 3.
IPCP down on circuit 3.
LCP down on circuit 3.
# 75: mm/dd/yy 14:15:57.035 INFO SLOT 2 SYNC Code: 13
Connector COM2 LLC1 service withdrawn.
```

The following message is normal after a dial-on-demand connection terminates:

```
# 76: mm/dd/yy 14:15:57.039 DEBUG SLOT 2 SWSERV Code: 46
Demand line failed for circuit 3.
sw_dd_line_fail set in use circuit to zero for com 2.
```

The router completes the orderly termination of the dial-on-demand link by re-initializing the port.

```
# 77: mm/dd/yy 14:15:57.054 INFO SLOT 2 SYNC Code: 9
Connector COM2 enabled.
# 78: mm/dd/yy 14:15:57.364 DEBUG SLOT 2 SYNC Code: 16
Connector COM2 initialization complete
Environment address - 3051f040 Line record address - 3052d8bc
Hardware map address - 30514f9c Initialization block -
80007800
Receive descriptor ring - 80005000 Transmit descriptor ring -
80005800
# 79: mm/dd/yy 14:15:57.364 DEBUG SLOT 2 PCAP Code: 67
interface became local - line 202102
# 80: mm/dd/yy 14:15:57.368 DEBUG SLOT 2 PCAP Code: 68
intf gate spawned - line 202102
```

The router returns to a “wait state,” where it is waiting for data.

```
# 81: mm/dd/yy 14:15:57.372 DEBUG SLOT 2 PCAP Code: 65
wait_state - line 202102
# 82: mm/dd/yy 14:15:58.401 DEBUG SLOT 2 SWSERV Code: 46
Connector COM2: FSM State: RDTR_DISCONNECTED(0)
```

```
Connector COM2: FSM Event: RDTR_EVENT_CCT_UP(1); isdn flags: 0x0
#    83: mm/dd/yy 14:15:58.401 INFO      SLOT 2 MODEMIF  Code: 22
Connector COM2: enable requested on cct 65535
Connector COM2: Starting, raise dtr mode, is modem connected and turned
on?
Connector COM2: Circuit has been brought up.
```

Dial-on-Demand V.25bis

The following log shows a successful dial-on-demand connection between the COM1 port in slot 2 and a modem configured for V.25bis.

These messages appear only when you click on the port configured for dial-on-demand, and set the Debug option under the Modem definition to Enabled. If you are using the Technician Interface, set attribute #29 (the debug attribute) of the object wfModemIfEntry to 1 (1 = enabled, 2 = disabled). The Debug option is available with router software Version 8.01 and later.

The following message indicates that the Sync software module enabled the COM1 port:

```
#      9: mm/dd/yy 13:07:24.725  INFO      SLOT  2  SYNC   Code:   9
Connector COM1 enabled.
```

The port completes initialization.

```
#      10: mm/dd/yy 13:07:24.995  DEBUG      SLOT  2  SYNC   Code:  16
Connector COM1 initialization complete
      Environment address      - 3051ea30 Line record address      - 3052e03c
      Hardware map address     - 30526e3c Initialization block      -
80007c00
      Receive descriptor ring - 80006000 Transmit descriptor ring -
80006800
#      11: mm/dd/yy 13:07:24.995  DEBUG      SLOT  2  PCAP   Code:  67
interface became local - line 202101
intf gate spawned - line 202101
#      12: mm/dd/yy 13:07:25.002  DEBUG      SLOT  2  PCAP   Code:  65
wait_state - line 202101
```

The FSM messages indicate that the modem and the router are communicating. The first FSM message shows the state the router was in when the FSM Event that follows occurred.

```
#      13: mm/dd/yy 13:07:26.031  DEBUG      SLOT  2  SWSERV  Code:  46
Connector COM1: FSM State: V25BIS_DISCONNECTED(0)
Connector COM1: FSM Event: V25BIS_EVENT_CCT_UP(1); isdn flags: 0x0
```


The port uses the CTS (clear to send) pin signal to determine whether a modem is present.

```
# 14: mm/dd/yy 13:07:26.031 INFO      SLOT 2 MODEMIF  Code: 22
Connector COM1: enable requested on cct 65535
```

The circuit number 65535 does not activate until data is waiting to transmit across the link.

The FSM messages indicate that the modem and the router are communicating. The first FSM message shows the state the router was in when the FSM Event that follows occurred.

```
# 15: mm/dd/yy 13:07:26.591 DEBUG     SLOT 2 SWSERV   Code: 46
Connector COM1: FSM State: V25BIS_WAIT_FOR_CTS(1)
Connector COM1: FSM Event: V25BIS_EVENT_CTS_UP(5); isdn flags: 0x1
# 16: mm/dd/yy 13:07:26.591 TRACE     SLOT 2 MODEMIF  Code: 53
Connector COM1: CTS has come up.
```

The router believes a V.25bis modem is present because it detected a CTS signal. The following message indicates that you configured the port for V.25bis, rather than Raise DTR.

```
# 17: mm/dd/yy 13:07:26.591 DEBUG     SLOT 2 MODEMIF  Code: 9
Connector COM1: modem present V.25bis mode
# 18: mm/dd/yy 13:07:26.591 DEBUG     SLOT 2 SWSERV   Code: 46
Line Mgr received line ready for line 1
# 19: mm/dd/yy 13:07:26.591 INFO      SLOT 2 SWSERV   Code: 10
Sync Line 1 available for dial on demand pool 1.
```

The router provides LLC service on the dial-on-demand port only after it detects a CTS signal.

```
# 20: mm/dd/yy 13:07:26.591 INFO      SLOT 2 SYNC    Code: 11
Connector COM1 providing LLC1 service.
```

The router pings the remote side of the dial-on-demand link to provide data to transmit across the link, and displays a “data received” message when it receives a response.

```
# 21: mm/dd/yy 13:09:16.174 INFO      SLOT 2 SWSERV   Code: 23
Data received for dial on demand circuit 2.
# 22: mm/dd/yy 13:09:16.178 DEBUG     SLOT 2 SWSERV   Code: 46
Connector COM1: FSM State: V25BIS_WAIT_DATA_OR_IND(2)
Connector COM1: FSM Event: V25BIS_EVENT_DATA_AVAIL(7); isdn flags: 0x9
# 23: mm/dd/yy 13:09:16.178 TRACE     SLOT 2 MODEMIF  Code: 34
Connector COM1: DATA Available.
# 24: mm/dd/yy 13:09:16.178 DEBUG     SLOT 2 SWSERV   Code: 44
```

```
SW Sent you are cc 2 message to line 1
The line is given a valid circuit number (2) in order to be activated
# 25: mm/dd/yy 13:09:16.193 INFO SLOT 2 SWSERV Code: 7
Dial on demand circuit being established on line 1.
```

The router forwards a call request number (CRN) to the V.25bis modem. It uses the phone number configured in the Outgoing field of the circuit definition.

```
# 26: mm/dd/yy 13:09:16.225 TRACE SLOT 2 MODEMIF Code: 35
Connector COM1: Sent CRN cmd to T3053
```

In this example, the cable connection to the modem is loose. The router fails to receive a response from the modem indicating that it received the CRN. The router exceeds its inactivity timeout threshold, and drops DTR to terminate the connection to the modem.

```
# 27: mm/dd/yy 13:10:17.446 DEBUG SLOT 2 SWSERV Code: 46
Connector COM1: FSM State: V25BIS_WAIT_FOR_ADAP_RSP(3)
Connector COM1: FSM Event: V25BIS_EVENT_TO(0); isdn flags: 0x4009
isdn_fsm_TO_WAIT - calling drop_dtr
# 28: mm/dd/yy 13:10:18.518 TRACE SLOT 2 MODEMIF Code: 27
Connector COM1: Connection timeout, retry in progress
# 29: mm/dd/yy 13:10:18.518 DEBUG SLOT 2 SWSERV Code: 46
Before g_delay for retry timer in - isdn_fsm_CONN_DELAY_IND
```

The router reinitializes the link with the modem after detecting that CTS is high.

```
# 30: mm/dd/yy 13:10:18.784 TRACE SLOT 2 MODEMIF Code: 53
Connector COM1: CTS has come up.
# 31: mm/dd/yy 13:10:18.784 DEBUG SLOT 2 MODEMIF Code: 9
Connector COM1: modem present V.25bis mode
```

Once again, the router sends the CRN to the modem.

```
# 32: mm/dd/yy 13:10:18.784 TRACE SLOT 2 MODEMIF Code: 35
Connector COM1: Sent CRN cmd to T3053
# 65: mm/dd/yy 13:12:58.985 TRACE SLOT 2 MODEMIF Code: 35
Connector COM1: Sent CRN cmd to T3053
# 66: mm/dd/yy 13:12:59.032 DEBUG SLOT 2 SWSERV Code: 46
Connector COM1: FSM State: V25BIS_WAIT_FOR_ADAP_RSP(3)
Connector COM1: FSM Event: V25BIS_EVENT_VALID_RSP(8); isdn flags: 0x4009
```

The messages assume that you reconnected the cable to the modem.

The router receives a response from the modem.

```
# 67: mm/dd/yy 13:12:59.032 TRACE SLOT 2 MODEMIF Code: 38
Connector COM1: Adapter accepted CRN command
```

The router now waits for the modem to raise DSR. It detects that the modem dropped CTS. The modem does this to prevent the router from sending more data until it establishes a connection with the remote modem.

```
# 68: mm/dd/yy 13:13:02.075  DEBUG    SLOT 2  SWSERV    Code 46
Connector COM1: FSM State: V25BIS_WAIT_FOR_DSR(5)
Connector COM1: FSM Event: V25BIS_EVENT_CTS_DN(6); isdn flags: 0x4008
# 69: mm/dd/yy 13:13:23.263  DEBUG    SLOT 2  SWSERV    Code: 46
Connector COM1: FSM State: V25BIS_WAIT_FOR_DSR(5)
```

The router receives a signal from the modem indicating that the connection between the modems is up.

```
# 70: mm/dd/yy 13:13:23.267  DEBUG    SLOT 2  SWSERV    Code 46
Connector COM1: FSM Event: V25BIS_EVENT_CONN_IND(11); isdn flags: 0x4008
# 71: mm/dd/yy 13:13:23.267  INFO     SLOT 2  MODEMIF   Code: 46
Connector COM1: Received a connect indication (CNX)
```

The modem raises DSR and CTS.

```
# 72: mm/dd/yy 13:13:23.673  DEBUG    SLOT 2  SWSERV    Code 46
Connector COM1: FSM State: V25BIS_WAIT_FOR_DSR(5)
Connector COM1: FSM Event: V25BIS_EVENT_CTS_UP(5); isdn flags: 0x4009
Connector COM1: FSM State: V25BIS_WAIT_FOR_DSR(5)
Connector COM1: FSM Event: V25BIS_EVENT_DSR_UP(3); isdn flags: 0x400b
```

The router determines that a successful connection is available between both routers connected via the dial-on-demand link.

```
# 73: mm/dd/yy 13:13:23.673  TRACE    SLOT 2  MODEMIF   Code 54
Connector COM1: DSR has come up.
# 74: mm/dd/yy 13:13:23.673  INFO     SLOT 2  MODEMIF   Code 31
Connector COM1: Connection established.
# 75: mm/dd/yy 13:13:23.677  TRACE    SLOT 2  PPP       Code: 43
Sending LCP Configure-Request on circuit 2.
# 76: mm/dd/yy 13:13:23.806  TRACE    SLOT 2  PPP       Code: 55
Received LCP Configure-Ack on circuit 2.
# 77: mm/dd/yy 13:13:25.930  TRACE    SLOT 2  PPP       Code: 54
Received LCP Configure-Request on circuit 2.
Sending LCP Configure-Ack on circuit 2.
# 78: mm/dd/yy 13:13:25.930  INFO     SLOT 2  PPP       Code: 38
Link Establishment Phase complete on circuit 2.
Starting Network Control Protocols on circuit 2.
```

The PPP link over the dial-on-demand circuit establishes an LCP connection. The IP software starts and establishes a connection over the dial-on-demand link.

```
# 79: mm/dd/yy 13:13:25.930  TRACE    SLOT 2  PPP       Code: 43
Sending IPCP Configure-Request on circuit 2.
```

```
# 80: mm/dd/yy 13:13:25.930 INFO      SLOT 2 PPP      Code: 28
LCP up on circuit 2.
# 81: mm/dd/yy 13:13:26.058 TRACE     SLOT 2 PPP      Code: 54
Received IPCP Configure-Request on circuit 2.
IPCP Naking IP-Address option value 0x0 with value 0x2020201 on circuit
2.
Sending IPCP Configure-Nak on circuit 2.
# 84: mm/dd/yy 13:13:26.094 TRACE     SLOT 2 PPP      Code: 55
Received IPCP Configure-Ack on circuit 2.
# 85: mm/dd/yy 13:13:26.220 TRACE     SLOT 2 PPP      Code: 54
Received IPCP Configure-Request on circuit 2.
# 86: mm/dd/yy 13:13:26.224 TRACE     SLOT 2 PPP      Code: 44
Sending IPCP Configure-Ack on circuit 2.
# 87: mm/dd/yy 13:13:26.224 INFO      SLOT 2 PPP      Code: 28
IPCP up on circuit 2.
```

The protocol on top of the dial-on-demand link is active. The V.25bis communication ends. The modem dropped the DSR signal to the router, and the router in turn dropped DTR to terminate the connection to the modem. ULI stands for upper-layer indication.

```
# 88: mm/dd/yy 13:13:26.224 DEBUG     SLOT 2 SWSERV   Code: 46
Connector COM1: FSM State: V25BIS_WAIT_FOR_ULI(6)
# 89: mm/dd/yy 13:13:26.228 DEBUG     SLOT 2 SWSERV   Code: 46
Connector COM1: FSM Event: V25BIS_EVENT_ULI_IND(15); isdn flags: 0x420b
# 90: mm/dd/yy 13:13:51.529 DEBUG     SLOT 2 SWSERV   Code: 46
Connector COM1: FSM State: V25BIS_CONNECTED(7)
Connector COM1: FSM Event: V25BIS_EVENT_DSR_DN(4); isdn flags: 0x4201
# 91: mm/dd/yy 13:13:51.529 TRACE     SLOT 2 MODEMIF   Code: 32
Connector COM1: DSR lost connection closed.
# 92: mm/dd/yy 13:13:51.529 DEBUG     SLOT 2 SWSERV   Code: 46
isdn_down_cct - calling drop_dtr
# 93: mm/dd/yy 13:13:51.529 INFO      SLOT 2 PPP      Code: 31
Stopping Network Control Protocols on circuit 2.
IPCP down on circuit 2.
LCP down on circuit 2.
# 94: mm/dd/yy 13:13:51.552 INFO      SLOT 2 SYNC     Code: 13
Connector COM1 LLC1 service withdrawn.
```

The following message is normal after a dial-on-demand connection terminates:

```
# 95: mm/dd/yy 13:13:51.556 DEBUG     SLOT 2 SWSERV   Code: 46
Demand line failed for circuit 2.
sw_dd_line_fail set in use circuit to zero for com 1.
```

The router completes the orderly termination of the dial-on-demand link by re-initializing the port.

```
# 96: mm/dd/yy 13:13:51.572 INFO SLOT 2 SYNC Code: 9
Connector COM1 enabled.
# 97: mm/dd/yy 13:13:51.841 DEBUG SLOT 2 SYNC Code: 16
Connector COM1 initialization complete
Environment address - 3051ea30 Line record address - 3052e03c
Hardware map address - 30526e3c Initialization block -
80007c00
Receive descriptor ring - 80006000 Transmit descriptor ring -
80006800
# 98: mm/dd/yy 13:13:51.841 DEBUG SLOT 2 PCAP Code: 67
interface became local - line 202101
intf gate spawned - line 202101
# 99: mm/dd/yy 13:13:51.849 DEBUG SLOT 2 PCAP Code: 65
wait_state - line 202101
# 100: mm/dd/yy 13:13:52.846 DEBUG SLOT 2 SWSERV Code: 46
Connector COM1: FSM State: V25BIS_DISCONNECTED(0)
Connector COM1: FSM Event: V25BIS_EVENT_CCT_UP(1); isdn flags: 0x0
# 101: mm/dd/yy 13:13:52.846 INFO SLOT 2 MODEMIF Code: 22
Connector COM1: enable requested on cct 65535
# 102: mm/dd/yy 13:13:53.406 DEBUG SLOT 2 SWSERV Code: 46
Connector COM1: FSM State: V25BIS_WAIT_FOR_CTS(1)
Connector COM1: FSM Event: V25BIS_EVENT_CTS_UP(5); isdn flags: 0x1
# 103: mm/dd/yy 13:13:53.406 TRACE SLOT 2 MODEMIF Code: 53
Connector COM1: CTS has come up.
# 104: mm/dd/yy 13:13:53.406 DEBUG SLOT 2 MODEMIF Code: 9
Connector COM1: modem present V.25bis mode
# 105: mm/dd/yy 13:13:53.406 DEBUG SLOT 2 SWSERV Code: 46
Line Mgr received line ready for line 1
# 106: mm/dd/yy 13:13:53.406 INFO SLOT 2 SWSERV Code: 10
Sync Line 1 available for dial on demand pool 1.
# 107: mm/dd/yy 13:13:53.406 INFO SLOT 2 SYNC Code: 11
Connector COM1 providing LLC1 service.
```

MCT1 Log Information in a Lab Environment

The log messages in this section show what happens when you access the MCT1 Line Tests option. In the sample display, port 2 of an MCT1-2 installed in slot 5 is sending a payload loopback to port 1 of an MCT1-2 in slot 4. See *Configuring WAN Line Services* for information about testing MCT1 lines.

When you enter the Technician Interface script command **show ds1e1 port**, the Technician Interface displays the MCT1-2 port setup, as follows:

```
[3:1]$ show ds1e1 port
DS1E1 Port Status:
-----
```

Slot	Conn	State	MTU	Loopback State	Accept Loopback	BERT Mode	Line Type	Line Coding	FDL Type	FDL Addr
4	1	Loopback	1600	Net Payload	Enabled	Off	ESF	B8ZS	ANSI	BY
5	2	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY

2 entries in table.

When the remote slot (slot 4) receives a loop-up or loop-down command, the remote yellow loopback LED lights on port 1 in slot 4, and the following messages appear in the log:

```
# 2: mm/dd/yy 08:56:17.563 INFO SLOT 4 DS1E1 Code: 55
Connector COM2 received loop-up code
# 18: mm/dd/yy 09:08:47.872 INFO SLOT 4 DS1E1 Code: 56
Connector COM2 received loop-down code
# 3: mm/dd/yy 10:31:12.638 INFO SLOT 2 MIB Code: 5
wfdsl1e1ActionEntry.5.905102 set to 5
# 4: mm/dd/yy 10:31:12.683 INFO SLOT 4 DS1E1 Code: 30
Connector COM1 Unscheduled FDL message - Payload Loopback Activate.
# 5: mm/dd/yy 10:31:12.687 INFO SLOT 4 DS1E1 Code: 22
Connector COM1, Logical Line 1 LLC service withdrawn.
# 6: mm/dd/yy 10:31:33.105 WARNING SLOT 5 DS1E1 Code: 4
Connector COM2, Logical Line 1 receiver timeout.
# 7: mm/dd/yy 10:31:33.109 DEBUG SLOT 5 DP Code: 23
dp_line_map - Line GH 0x8400b4e3 died, cct 3
# 8: mm/dd/yy 10:31:33.113 INFO SLOT 5 DS1E1 Code: 22
Connector COM2, Logical Line 1 LLC service withdrawn.
# 9: mm/dd/yy 10:31:33.113 DEBUG SLOT 5 DP Code: 41
LINE_DOWN msg rcvd for line gate 0x400b4e3 on cct 3.
```

```
Found dead line 0x400b4e3 at offset 0
Last line 0x400b4e3 in cct 3 died, killing circuit gate
DP killing CC gate for cct 3.
# 10: mm/dd/yy 10:31:33.124 INFO SLOT 5 IP Code: 3
Interface 4.1.2.1 down on circuit 3
# 11: mm/dd/yy 10:31:33.148 INFO SLOT 5 DP Code: 2
Circuit 3 down.
# 14: mm/dd/yy 10:31:33.164 DEBUG SLOT 5 GAME Code: 84
FWD [ 5-60f0] (84000053->bc000403): down=3c000000, no_ACK=00000000,
NAK=3c000000
# 15: mm/dd/yy 10:31:33.230 DEBUG SLOT 5 DS1E1 Code: 50
Connector COM2, Logical Line 1 time_slot = 1.
Connector COM2, Logical Line 1 time_slot = 2.
Connector COM2, Logical Line 1 time_slot = 3.
Connector COM2, Logical Line 1 time_slot = 4.
Connector COM2, Logical Line 1 time_slot = 5.
Connector COM2, Logical Line 1 time_slot = 6.
Connector COM2, Logical Line 1 time_slot = 7.
# 16: mm/dd/yy 10:31:33.234 DEBUG SLOT 5 DS1E1 Code: 50
Connector COM2, Logical Line 1 time_slot = 8.
Connector COM2, Logical Line 1 time_slot = 9.
Connector COM2, Logical Line 1 time_slot = 10.
Connector COM2, Logical Line 1 time_slot = 11.
Connector COM2, Logical Line 1 time_slot = 12.
Connector COM2, Logical Line 1 time_slot = 13.
Connector COM2, Logical Line 1 time_slot = 14.
Connector COM2, Logical Line 1 time_slot = 15.
Connector COM2, Logical Line 1 time_slot = 16.
Connector COM2, Logical Line 1 time_slot = 17.
Connector COM2, Logical Line 1 time_slot = 18.
Connector COM2, Logical Line 1 time_slot = 19.
Connector COM2, Logical Line 1 time_slot = 20.
Connector COM2, Logical Line 1 time_slot = 21.
# 17: mm/dd/yy 10:31:33.238 DEBUG SLOT 5 DS1E1 Code: 50
Connector COM2, Logical Line 1 time_slot = 22.
Connector COM2, Logical Line 1 time_slot = 23.
Connector COM2, Logical Line 1 time_slot = 24.
Connector COM2, Logical Line 1 initialization complete
Environment address - 30675250 Line record address - 307326ac
Hardware map address - 3072f784 Initialization block - 80006c00
Receive descriptor ring - 80002600 Transmit descriptor ring -
80005200
# 18: mm/dd/yy 10:31:58.218 DEBUG SLOT 5 PCAP Code: 67
interface became local - line 10905102
intf gate spawned - line 10905102
wait_state - line 10905102
```

To disable payload loopback, click on FDL Disable Payload in the Line Tests window. (FDL stands for facility data link.) The loopback LED turns off on port 1 in slot 4, and the log displays the following messages:

```
[3:1]$ log -fftwid
# 1: mm/dd/yy 10:38:29.007 INFO SLOT 3 TI Code: 3
Log cleared !
# 2: mm/dd/yy 10:38:39.239 INFO SLOT 2 MIB Code: 7
wfSrmnp.3.0 set to 192.32.18.9
# 3: mm/dd/yy 10:38:39.297 INFO SLOT 2 MIB Code: 5
wfDs1e1ActionEntry.5.905102 set to 6
# 4: mm/dd/yy 10:38:39.312 INFO SLOT 4 DS1E1 Code: 31
Connector COM1 Unscheduled FDL message received - type Payload Loopback
Deactivate.
# 5: mm/dd/yy 10:38:39.355 DEBUG SLOT 4 DS1E1 Code: 50
Connector COM1, Logical Line 1 time_slot = 1.
# 6: mm/dd/yy 10:38:39.359 DEBUG SLOT 4 DS1E1 Code: 50
Connector COM1, Logical Line 1 time_slot = 2.
Connector COM1, Logical Line 1 time_slot = 3.
Connector COM1, Logical Line 1 time_slot = 4.
Connector COM1, Logical Line 1 time_slot = 5.
Connector COM1, Logical Line 1 time_slot = 6.
Connector COM1, Logical Line 1 time_slot = 7.
Connector COM1, Logical Line 1 time_slot = 8.
Connector COM1, Logical Line 1 time_slot = 9.
Connector COM1, Logical Line 1 time_slot = 10.
Connector COM1, Logical Line 1 time_slot = 11.
Connector COM1, Logical Line 1 time_slot = 12.
Connector COM1, Logical Line 1 time_slot = 13.
Connector COM1, Logical Line 1 time_slot = 14.
Connector COM1, Logical Line 1 time_slot = 15.
# 7: mm/dd/yy 10:38:39.363 DEBUG SLOT 4 DS1E1 Code: 50
Connector COM1, Logical Line 1 time_slot = 16.
Connector COM1, Logical Line 1 time_slot = 17.
Connector COM1, Logical Line 1 time_slot = 18.
Connector COM1, Logical Line 1 time_slot = 19.
Connector COM1, Logical Line 1 time_slot = 20.
Connector COM1, Logical Line 1 time_slot = 21.
Connector COM1, Logical Line 1 time_slot = 22.
Connector COM1, Logical Line 1 time_slot = 23.
Connector COM1, Logical Line 1 time_slot = 24.
Connector COM1, Logical Line 1 initialization complete
Environment address - 30ea8ba0 Line record address - 30f30dc4
Hardware map address - 30f2da34 Initialization block - 80006800
Receive descriptor ring - 80001000 Transmit descriptor ring -
80003c00
```



```
# 8: mm/dd/yy 10:38:39.367  DEBUG      SLOT  4  PCAP      Code:  67
interface became local - line 10904101
intf gate spawned - line 10904101
# 9: mm/dd/yy 10:38:39.371  DEBUG      SLOT  4  PCAP      Code:  65
wait_state - line 10904101
# 10: mm/dd/yy 10:38:44.351  DEBUG      SLOT  5  DP        Code:  67
Missing Circuit Options record cct #3.
DP gate rcv'd LINE message for cct 3.
# 11: mm/dd/yy 10:38:44.355  DEBUG      SLOT  5  DP        Code:  23
Creating Circuit 3 soloist with line GH 0xb381
# 12: mm/dd/yy 10:38:44.355  DEBUG      SLOT  5  GAME      Code:  23
SOLO (0x00403): election opening 3c000000/3c000000 (3c000000)
vote=00000000
# 13: mm/dd/yy 10:38:44.386  DEBUG      SLOT  5  GAME      Code:  97
SOLO (0x00403): election WON 0x04000000 (repl=bc000009/3c000000)
SOLO (0x00403): election CLOSING 3c000000/3c000000 (3c000000)
vote=00000000
# 14: mm/dd/yy 10:38:44.390  INFO       SLOT  5  ARP       Code:   1
Service is up on circuit 3
```

The following command displays the new port status:

```
[3:1]$ show ds1e1 port
```

```
DS1E1 Port Status:
```

```
-----
```

Slot	Conn	State	MTU	Loopback State	Accept Loopback	BERT Mode	Line Type	Line Coding	FDL Type	FDL Addr
4	1	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY
5	2	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY

2 entries in table.

If you click on a test option (FDL Line Loop CI, IA, or IB), the following messages appear:

```
# 3: mm/dd/yy 10:43:14.207  INFO       SLOT  2  MIB       Code:   5
wfDs1E1ActionEntry.5.905102 set to 1
# 4: mm/dd/yy 10:43:14.207  INFO       SLOT  5  DS1E1     Code:  22
Connector COM2, Logical Line 1 LLC service withdrawn.
# 5: mm/dd/yy 10:43:14.238  INFO       SLOT  4  DS1E1     Code:  27
Connector COM1 Unscheduled FDL message received - type Line Loopback
Activate.
```

If you click on the FDL Disable Line Loop option, the LED turns off and the following log messages appear:

```
#    3: mm/dd/yy 10:46:19.624  INFO      SLOT  2  MIB      Code:   5
wfDs1E1ActionEntry.5.905102 set to 6
#    4: mm/dd/yy 10:48:24.391  INFO      SLOT  2  MIB      Code:   7
wfSnmp.3.0 set to 0.0.0.0
#    5: mm/dd/yy 10:48:24.454  DEBUG     SLOT  2  SNMP     Code:  35
Agent cleared lock.
#    6: mm/dd/yy 10:49:10.786  INFO      SLOT  2  MIB      Code:   7
wfSnmp.3.0 set to 192.32.18.9
#    7: mm/dd/yy 10:49:10.849  INFO      SLOT  2  MIB      Code:   5
wfDs1E1ActionEntry.5.905102 set to 4
#    8: mm/dd/yy 10:49:10.867  INFO      SLOT  4  DS1E1    Code:  28
Connector COM1 Unscheduled FDL message received - type Line Loopback
Deactivate.
#    9: mm/dd/yy 10:49:10.910  DEBUG     SLOT  4  DS1E1    Code:  50
Connector COM1, Logical Line 1 time_slot = 1.
```

The following command displays the new port status:

```
[3:1]$ show ds1e1 port
DS1E1 Port Status:
-----
```

Slot	Conn	State	MTU	Loopback State	Accept Loopback	BERT Mode	Line Type	Line Coding	FDL Type	FDL Addr
4	1	Loopback	1600	Net Line	Enabled	Off	ESF	B8ZS	ANSI	BY
5	2	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY

2 entries in table.

The loopback LED lights. The following command displays the new port status:

```
[3:1]$ show ds1e1 port
DS1E1 Port Status:
-----
```

Slot	Conn	State	MTU	Loopback State	Accept Loopback	BERT Mode	Line Type	Line Coding	FDL Type	FDL Addr
4	1	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY
5	2	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY

The same unscheduled message shown in line 8 earlier applies to FDL line loops IA and IB.

If you click on FDL Disable ALL, the MIB entity disables all FDL line loops. It sends a Universal Loopback Deactivate message.

```
# 16: mm/dd/yy 10:58:54.840 INFO SLOT 2 MIB Code: 5
wfDs1E1ActionEntry.5.905102 set to 7
# 17: mm/dd/yy 10:58:54.871 INFO SLOT 4 DS1E1 Code: 32
Connector COM1 Unscheduled FDL message received - type Universal
Loopback Deactivate.
```

If you click on Loop Up, the line goes into a loopback state. The only visible evidence of this state is that the loopback LED lights. The log shows the following:

```
# 2: mm/dd/yy 11:02:41.489 INFO SLOT 2 MIB Code: 7
wfSnmp.3.0 set to 192.32.18.9
# 3: mm/dd/yy 11:02:41.552 INFO SLOT 2 MIB Code: 5
wfDs1E1ActionEntry.4.905102 set to 1
# 4: mm/dd/yy 11:02:47.292 INFO SLOT 4 DS1E1 Code: 22
Connector COM1, Logical Line 1 LLC service withdrawn.
```

The following command displays the new port status:

```
[3:1]$ show ds1e1 port
DS1E1 Port Status:
-----
```

Slot	Conn	State	MTU	Loopback State	Accept Loopback	BERT Mode	Line Type	Line Coding	FDL Type	FDL Addr
4	1	Loopback	1600	Net Line	Enabled	Off	ESF	B8ZS	ANSI	BY
5	2	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY

2 entries in table.

If you click on Loop Down, the MIB entity disables the line loopback and the log shows the following:

```
[3:1]$ log -fftwid
# 2: mm/dd/yy 11:06:25.815 INFO SLOT 2 MIB Code: 7
wfSnmp.3.0 set to 192.32.18.9
# 3: mm/dd/yy 11:06:25.918 INFO SLOT 2 MIB Code: 5
wfDs1E1ActionEntry.4.905102 set to 2
# 4: mm/dd/yy 11:06:31.675 DEBUG SLOT 4 DS1E1 Code: 50
Connector COM1, Logical Line 1 time_slot = 1.
Connector COM1, Logical Line 1 time_slot = 2.
```

```

Connector COM1, Logical Line 1 time_slot = 3.
Connector COM1, Logical Line 1 time_slot = 4.
Connector COM1, Logical Line 1 time_slot = 5.
Connector COM1, Logical Line 1 time_slot = 6.
Connector COM1, Logical Line 1 time_slot = 7.
Connector COM1, Logical Line 1 time_slot = 8.
Connector COM1, Logical Line 1 time_slot = 9.
Connector COM1, Logical Line 1 time_slot = 10.
# 5: mm/dd/yy 11:06:31.679 DEBUG SLOT 4 DS1E1 Code: 50
Connector COM1, Logical Line 1 time_slot = 11.
Connector COM1, Logical Line 1 time_slot = 12.
Connector COM1, Logical Line 1 time_slot = 13.
Connector COM1, Logical Line 1 time_slot = 14.
Connector COM1, Logical Line 1 time_slot = 15.
Connector COM1, Logical Line 1 time_slot = 16.
Connector COM1, Logical Line 1 time_slot = 17.
Connector COM1, Logical Line 1 time_slot = 18.
Connector COM1, Logical Line 1 time_slot = 19.
Connector COM1, Logical Line 1 time_slot = 20.
Connector COM1, Logical Line 1 time_slot = 21.
Connector COM1, Logical Line 1 time_slot = 22.
Connector COM1, Logical Line 1 time_slot = 23.
Connector COM1, Logical Line 1 time_slot = 24.
# 6: mm/dd/yy 11:06:31.683 DEBUG SLOT 4 DS1E1 Code: 39
Connector COM1, Logical Line 1 initialization complete
Environment address - 30 - ea7ba0 Line record address -30f30dc4
Hardware map address - 30f2da34 Initialization block - 80006800
Receive descriptor ring - 80001000 Transmit descriptor ring - 80003c00

```

The following command displays the new port status:

```

[3:1]$ show ds1e1 port
DS1E1 Port Status:
-----

```

Slot	Conn	State	MTU	Loopback State	Accept Loopback	BERT Mode	Line Type	Line Coding	FDL Type	FDL Addr
4	1	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY
5	2	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY

2 entries in table.

If you change the setting of the Line Type parameter from ESF (extended super frame) to SF (super frame), the following messages appear:

```

[3:1]$ s wfDs1E1ConfigEntry.wfDs1E1ConfigLineType.904101 3;commit

```

```
[3:1]$ s wfDs1E1ConfigEntry.wfDs1E1ConfigLineType.905102 3;commit
```

The following command displays the new port status:

```
[3:1]$ show ds1e1 port
```

```
DS1E1 Port Status:
```

```
-----
```

Slot	Conn	State	MTU	Loopback State	Accept Loopback	BERT Mode	Line Type	Line Coding	FDL Type	FDL Addr
4	1	Yel Alarm	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY
5	2	Yel Alarm	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY

```
2 entries in table.
```

```
[3:1]$ !
```

```
DS1E1 Port Status:
```

```
-----
```

Slot	Conn	State	MTU	Loopback State	Accept Loopback	BERT Mode	Line Type	Line Coding	FDL Type	FDL Addr
4	1	Yel Alarm	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY
5	2	Up	1600	No Loop	Enabled	Off	ESF	B8ZS	ANSI	BY

```
2 entries in table.
```

If you set the port line type to AMI (alternate mark inversion), the following messages appear:

```
# 7: mm/dd/yy 11:25:03.226 WARNING SLOT 4 DS1E1 Code: 14
Connector COM1 Loss of signal failure.
# 8: mm/dd/yy 11:25:03.226 INFO SLOT 4 DS1E1 Code: 22
Connector COM1, Logical Line 1 LLC service withdrawn.
# 9: mm/dd/yy 11:25:03.335 INFO SLOT 4 DS1E1 Code: 24
Connector COM1 B8ZS code received on port configured for AMI.
# 10: mm/dd/yy 11:25:05.343 WARNING SLOT 5 DS1E1 Code: 17
Connector COM2 Remote alarm indication failure.
```

The following command displays the new port status:

```
[3:1]$ show ds1e1 port
```

```
DS1E1 Port Status:
```

```
-----
```

Slot	Conn	State	MTU	Loopback State	Accept Loopback	BERT Mode	Line Type	Line Coding	FDL Type	FDL Addr
4	1	Red Alarm	1600	No Loop	Enabled	Off	ESF	AMI	AT&T	BY
5	2	Red Alarm	1600	No Loop	Enabled	Off	ESF	AMI	AT&T	BY

2 entries in table.

If you configure the primary clock source as the port 2 loop and the secondary clock source as the port 1 loop, both clocks fail and the following messages appear in the log:

```
# 62: mm/dd/yy 10:44:50.734 WARNING SLOT 3 DS1E1 Code: 14
Connector COM2 Loss of signal failure.
# 63: mm/dd/yy 10:44:50.734 INFO SLOT 3 DS1E1 Code: 23
Primary and Sec clocks unoperational - Switching to Internal Clock
Source.
```

The following message appears if you mismatch the line coding. In this example, the line coding of one side is AMI and the other is B8ZS (binary 8 zero substitution).

```
# 234: mm/dd/yy 09:01:43.121 INFO SLOT 2 DS1E1 Code: 24
Connector COM1 B8ZS code received on port configured for AMI.
```

If you set the line type to ESF, many messages indicate bipolar violations on the side configured for AMI.

```
Ti prompt> show ds1e1 fdl ansi1
DS1E1 Facility Data Link (FDL) errors (first half) - ANSI-403 mode:
-----
```

Slot	Conn	CRC Counts	BPV Counts	OOF Counts	FE Counts	ES Counts
2	1	65535	964252	0	0	1675

Appendix B

Using the Technician Interface to Configure and Run Packet Capture

This appendix describes how to use the Technician Interface to configure and run the Packet Capture utility.

Topic	Page
Overview	B-2
Implementation Notes	B-4
Getting Started	B-5
Using Optional Features	B-18
Configuration Examples	B-27
Displaying the Current Packet Capture Configuration Settings	B-30
Displaying Event Messages Issued by Packet Capture	B-31
Using a Sun Workstation or DOS PC to Display Packets	B-31
Converting a Packet Capture File to Network General Sniffer Format	B-36
Reference Guide to Packet Capture	B-38

Overview

Packet Capture allows you to examine packets passing through selected circuits on a Bay Networks router. It copies the packets from the circuits to a file in the router's memory. You can then open the file and view the packets to troubleshoot a problem.

The following routers and physical media services support Packet Capture:

- Routers: AN, ANH, AFN, ARN, ASN, ALN, FN, LN, CN, BLN, BLN-2, BCN
- Physical media services: CSMA/CD (Ethernet), synchronous, T1, E1, MCT1, token ring, FDDI, HSSI, ISDN

You can use Packet Capture to do the following:

- Copy all incoming packets, outgoing packets, or both.
- Filter and copy incoming packets, outgoing packets, or both.
- Filter incoming packets, outgoing packets, or both, and copy only selected contents of those packets.

You can terminate Packet Capture as follows:

- Enter a command to terminate it immediately.
- Configure it to terminate itself when the Packet Capture file is full.
- Configure it to terminate itself when it matches a portion of an incoming or outgoing packet to a hexadecimal number or character string that you specify.

After Packet Capture terminates, you must choose a method to examine the file. Select the option in the following list that identifies the tools that you have available:

1. Establish a remote connection to the router using Optivity Internetwork 6.1 or later; then, use Network Tap to transfer a copy of the Packet Capture file and display the packets in hexadecimal, summary, or decoded format.

The decoded format identifies each field in the packet and, where appropriate, displays its contents in English. It also allows you to search packets for character strings.

See *Using Optivity Network Management System 8.0 Internetwork Applications* for Network Tap instructions.

2. Establish a remote connection to the router using FTP, TFTP, XMODEM, or the Network Tap application; then, use a Network General Sniffer to convert the file for processing.
 - a. Transfer a copy of the Packet Capture file from the router to a UNIX workstation or DOS PC.

See Using Optivity Network Management System 8.0 Internetwork Applications for Network Tap instructions.
 - b. Convert the file for processing by a Network General Sniffer using one of the following methods:
 - On a UNIX workstation, use Network Tap.
 - On a Sun workstation or DOS PC, use the Packet Convert utility. See [“Converting a Packet Capture File to Network General Sniffer Format”](#) on [page B-36](#).
 - c. Save the converted file on a DOS-formatted diskette and insert the diskette in a Network General Sniffer for analysis. See the Network General Sniffer manual to learn how to read the file.
3. Establish a local or out-of-band connection to the router using the Technician Interface; then, use the Technician Interface to decode and display the hexadecimal content of the packets.

The Technician Interface shows the following information about each packet:

- The sequential number of the packet in the file
- The date and time Packet Capture copied the packet
- The media carrying the packet
- The original size of the packet
- The direction of the packet (received for incoming, or transmitted for outgoing)
- The contents of the packet in hexadecimal format.

The Technician Interface also allows you to do the following:

- Identify the first packet you want to display by specifying its sequence number in the Packet Capture file.
- Limit the number of packets displayed.

4. Establish an FTP, TFTP, or XMODEM connection to the router from a DOS PC or Sun workstation to transfer a copy of the file; then, use the Packet Dump utility to display the packets in hexadecimal format.

See [“Using a Sun Workstation or DOS PC to Display Packets”](#) on [page B-31](#).

The Packet Dump utility shows the same information about each packet as the Technician Interface, but it does not provide options for specifying the packet by number or quantity.

See [“Displaying the File with Packet Dump”](#) on [page B-35](#).

Implementation Notes

Packet Capture copies only packets that are error free; it does not copy packets containing errors.

Packet Capture saves the MAC addresses in native media format.

Packet Capture does not display frame check sequence (FCS) fields.

On a BayStack ARN router, Packet Capture prompts for the module number of the interface. Specify 1 for synchronous interfaces. For interfaces that are configured with a WAN service other than synchronous (for example, BOT or ISDN interfaces), use the module number listed in [Table B-1](#).

Table B-1. Packet Capture Module Numbers for ARN Interfaces (Except Synchronous)

ARN Interface	Module Number for Packet Capture
Base module (XCVR1 or TOKEN1)	1
First WAN adapter module interface (COM1 or ISDN1)	2
Second WAN adapter module interface (COM2 or ISDN2)	3
Expansion module interface (XCVR2, TOKEN2, or COM3 to COM5)	4

Getting Started

This section describes how to start and stop Packet Capture and look at a Packet Capture file. The default parameter values allow Packet Capture to copy all incoming packets from the circuits you specify until you enter a command to terminate it. After learning the basic features of Packet Capture, you can go to [“Using Optional Features”](#) to customize Packet Capture.

The following sections provide basic instructions for using Packet Capture:

- [“Preparing Packet Capture to Run”](#)
- [“Starting Packet Capture”](#)
- [“Terminating Packet Capture”](#)
- [“Using the Technician Interface to Display a Packet Capture File”](#)
- [“Deleting a Packet Capture Instance”](#)

Preparing Packet Capture to Run

The following sections provide the minimum number of instructions required to prepare Packet Capture to run:

- [“Assigning the Processors to Run Packet Capture”](#)
- [“Creating an Instance of Packet Capture”](#)
- [“Allocating Memory for the Packet Capture File”](#)
- [“Specifying the Number of Bytes in Each Packet to Copy”](#)
- [“Enabling Packet Capture”](#)

Assigning the Processors to Run Packet Capture

To assign processors to run Packet Capture, you determine which slots in the router contain the circuits from which you want to copy packets. Then, enter the following Technician Interface command to assign the processors:

```
set wfProtocols.26.0 <slot_mask>;commit
```

26 represents the wfPktCaptureLoad attribute (parameter).

<slot_mask> is a hexadecimal number representing one or more slots containing circuits or channels from which you want to copy packets.

If you want Packet Capture to copy packets from circuits in a single I/O module, use the associated slot mask listed in [Table B-2](#).

Table B-2. Determining the Slot Mask

Slot No.	Slot Mask
1	0x80000000
2	0x40000000
3	0x20000000
4	0x10000000
5	0x08000000
6	0x04000000
8	0x01000000
9	0x00800000
10	0x00400000
11	0x00200000
12	0x00100000
13	0x00080000
14	0x00040000

Example

To load Packet Capture on slot 2, enter the following command:

set wfProtocols.26.0 0x40000000;commit

If you want to copy packets from more than one circuit, and the circuits are on different I/O modules, add the hexadecimal values for the associated slots listed in [Table B-2](#), and use the sum as the slot mask.

Example

Capture packets from the I/O modules in slots 3, 4, 8, and 10 as follows:

1. Add the associated slot masks as follows:

Slot 3	0x20000000
Slot 4	0x10000000
Slot 8	0x01000000
Slot 10	0x00400000
	<hr/>
	0x31400000

2. Specify the sum in the set command as follows:

set wfProtocols.26.0 0x31400000;commit

Creating an Instance of Packet Capture

To create a Packet Capture record associated with a circuit or channel from which you want to copy packets, you reference the circuit's line number. A line number is a unique number used to identify a circuit. Site Manager creates a line number each time you add a circuit to the router's configuration.

When you create a Packet Capture record, it creates a set of default parameter values associated with the line number and stores them in the MIB. The standard MIB term for this type of record is "instance."

Refer to the instructions in the section that applies to you:

- [“Creating an Instance for MCT1”](#)
- [“Creating an Instance for Other Media”](#)

Creating an Instance for MCT1

MCT1 uses logical lines within a physical connector. Each MCT1 line number represents a logical line.

Get the number of the logical line from which you want to copy packets as follows:

1. **Enter the following Technician Interface command to display the base line number:**

get wfDs1E1PortMapEntry.4.<slot>.<connector>

4 represents the wfDs1E1PortMapLineNumber attribute (parameter).

Example

Enter the following command to get the base line number of connector 1 on an MCT1 I/O module in slot 2:

get wfDs1E1PortMapEntry.4.2.1

In this example, the response is as follows:

902101

2. **Enter the following command to display the logical line number:**

get wfLogicalLineEntry.7.<base_line_number>.<index>

7 represents the wfLogicalLineNumber attribute (parameter).

<base_line_number> is the response to the command you entered in step [1](#).

<index> is the position of the logical line on the circuit.

Example

Enter the following command to get the number of logical line 1 from the example in step 1:

get wfLogicalLineEntry.7.902101.1

In this example, the response is as follows:

10902101

3. **Enter the following command to create an instance:**

set wfPktCaptureEntry.1.<line_no.> 1;commit

The first **1** represents the wfPktCaptureDelete attribute.

<line_no.> is the response to the command you entered in step [2](#). To list the current line numbers associated with Packet Capture, enter the command

list instances wfPktCaptureEntry.

The second **1** represents the numeric code for “create.”

Example

Enter the following command to create an instance for logical line 10902101:

set wfPktCaptureEntry.1.10902101 1;commit

Creating an Instance for Other Media

Create an instance as follows:

1. **Find the media in the following list and enter the associated Technician Interface command to get the number of the logical line from which you want to copy packets.**



Note: Type the uppercase and lowercase characters exactly as they appear in these instructions.

- Bisynchronous
get wfBisyncEntry.13.<slot>.<connector>
13 represents the wfBisyncLineNumber attribute.
- Ethernet (CSMA/CD)
get wfCSMACDEntry.38.<slot>.<connector>
38 represents the wfCSMACDLineNumber attribute.
- Sync, T1, E1, or ISDN B channel
get wfSyncEntry.79.<slot>.<connector>
79 represents the wfSyncLineNumber attribute.
- Token ring
get wfTokenRingEntry.66.<slot>.<connector>
66 represents the wfTokenRingLineNumber attribute.
- FDDI
get wfFddiEntry.44.<slot>.<connector>
44 represents the wfFddiLineNumber attribute.

- HSSI

get wfHssiEntry.60.<slot>.<connector>

60 represents the wfHssiLineNumber attribute.

- ISDN B channel

get wfIsdnBriInterfaceEntry.8.<slot>.<connector>

8 represents the wfIsdnBriLineNumber attribute.

Example 1

Enter the following command to get the line number of a synchronous interface on slot 2, connector 1:

get wfSyncEntry.79.2.1

The response is as follows:

202101

Example 2

Enter the following command to get the line number of a FDDI interface:

get wfFddiEntry.44.2.1

The response is as follows:

602101

2. **Enter the following command to create an instance:**

set wfPktCaptureEntry.1.<line_no.> 1;commit

The first **1** represents the wfPktCaptureDelete attribute.

<line_no.> is the number displayed after you issued the **get** command in [“Creating an Instance of Packet Capture.”](#) To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

The second **1** represents the numeric code for “create.”

Example

Enter the following command to create an instance for line number 202101:

set wfPktCaptureEntry.1.202101 1;commit

Allocating Memory for the Packet Capture File

You must allocate memory to store the Packet Capture file in order to capture packets. By default, the Packet Capture file uses 0 bytes of memory.

Allocate memory to the Packet Capture file as follows:

1. **Enter the following command to display the maximum number of contiguous bytes available:**

get wfKernelEntry.6.<slot no.> <value>

6 represents the wfKernelMemoryMaxSegFree attribute.



Note: The allocation of memory varies. If the processors have memory restrictions, enter this command every 15 seconds for 2 to 3 minutes and record each response.

2. **Enter the following command to specify the size of the Packet Capture file stored in memory:**

set wfPktCaptureEntry.8.<line_no.> <value>;commit

- **8** represents the wfPktCaptureBufSize attribute.
- **<line_no.>** is the number displayed after you issued the **get** command in “[Creating an Instance of Packet Capture](#)” on [page B-7](#).

To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

- **<value>** is the number of KB of available contiguous memory, minus 200 KB. The value 1 represents 1024 bytes (1 KB) of memory allocated for the Packet Capture file; the value 2 represents 2 KB.

To calculate the value, subtract 200 KB from the lowest number displayed in response to the **get** command that you entered in [step 1](#); then, divide this number by 1024. The result is the maximum value that Bay Networks recommends that you enter.

The less memory you allocate to Packet Capture, the lower the chance that the processor will reset because of a memory problem. However, you do need to allocate enough memory to store the packets you want to capture.

If less than 200 KB of free memory remains after Packet Capture starts, it sends a warning message to the log. If errors occur after you start Packet Capture, stop it and allocate less memory.

Specifying the Number of Bytes in Each Packet to Copy

You must specify the number of bytes in each packet to copy to the Packet Capture file. If you want to use a Network General Sniffer to read a Packet Capture file, you must set the size of the packets to a value the Sniffer supports. The Sniffer currently supports the following values: 32, 64, 128, 256, and 512; they correspond to the Bay Networks router settings 1, 2, 4, 8, and 16.

Enter the following command to specify the number of bytes in each packet to copy to the Packet Capture file:

```
set wfPktCaptureEntry.9.<line_no.> <value>;commit
```

9 represents the wfPktCapturePktSize attribute.

<line_no.> is the number displayed after you issued the **get** command in “[Creating an Instance of Packet Capture](#).” To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

<value> is any number of 32-byte increments in the range 1 to 144. The value 1 represents 32 bytes to be saved; the value 144 represents 4608 bytes to be saved.

Enabling Packet Capture

Enter the following Technician Interface command to enable the Packet Capture utility:

```
set wfPktCaptureEntry.2.<line_no.> 1;commit
```

2 represents the wfPktCaptureDisable attribute.

<line_no.> is the number displayed after you issued the **get** command in “[Creating an Instance of Packet Capture](#).” To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

1 represents the numeric code for “enable.”

Example

Enter the following command to enable Packet Capture for line number 202101:

set wfPktCaptureEntry.2.202101 1;commit

Starting Packet Capture

Enter the following Technician Interface command to start Packet Capture:

set wfPktCaptureEntry.5.<line_no.> 1;commit

5 represents the wfPktCaptureControl attribute.

<line_no.> is the number displayed after you issued the **get** command in “[Creating an Instance of Packet Capture](#).” To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

1 represents the numeric code for “start.”

Example

Enter the following command to start Packet Capture for line number 202101:

set wfPktCaptureEntry.5.202101 1;commit

Go to the next section.

Terminating Packet Capture

You must terminate Packet Capture before you can display the packets. Enter the following Technician Interface command to terminate it:

set wfPktCaptureEntry.5.<line_no.> 2;commit

5 represents the wfPktCaptureControl attribute.

<line_no.> is the number displayed after you issued the **get** command in “[Creating an Instance of Packet Capture](#).” To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

2 represents the numeric code for “stop.”

Example

Enter the following command to enable Packet Capture for line number 202101:

set wfPktCaptureEntry.5.202101 2;commit

Go to the next section.

Using the Technician Interface to Display a Packet Capture File

Enter the following Technician Interface command to display a Packet Capture file stored in memory:

pktdump <line_no.> [-s<start>] [-c<count>]

<line_no.> is the number displayed after you issued the **get** command in “[Creating an Instance of Packet Capture](#).” To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

[-s<start>] and [-c<count>] are optional.

<start> is the number of the packet in the file to be displayed first. If you do not specify one, the Technician Interface displays the first packet in the file.

<count> is the number of packets to display in sequential order. If you do not specify one, the Technician Interface displays all packets.

If the Packet Capture file does not contain packets, the following message appears:

No packets captured for linenumber <line_no.>

If the Packet Capture file contains packets, the contents of each packet appear as follows:

- The first line shows information Packet Capture recorded about the packet. It includes the following:
 - The sequential number of the packet in the file
 - The date and time Packet Capture copied the packet
 - The media carrying the packet

If the media is Sync, the name of the protocol on the Sync interface appears instead of the media.

- The number of bytes in the packet
- The direction of the packet: Rx for incoming packets and Tx for outgoing packets
- The remaining lines show the data in the packet in hexadecimal format.

Example 1

Enter the following command to display all packets associated with line number 102101:

pkt dump 102101

```
Pkt# 1 mm/dd/yy 10:20:26.430 CSMACD 60 Rx
00000000: 01 80 c2 00 00 00 00 00 a3 00 00 0c 00 26 42 42
00000010: 03 00 00 00 00 00 80 00 00 00 a3 00 00 0c 00 00
00000020: 00 00 80 00 00 00 a3 00 00 0c 80 07 00 00 14 00
00000030: 02 00 0f 00 3f 09 ef df 00 00 01 00 00 00 00 00

Pkt# 2 mm/dd/yy 10:20:28.196 CSMACD 60 Rx
00000000: 00 00 a2 03 c1 66 00 00 a2 03 c1 66 81 02 01 01
00000010: 00 00 00 00 00 1f 80 00 00 00 a3 00 00 0c 00 00
00000020: 00 00 80 00 00 00 a3 00 00 0c 80 07 00 00 14 00
00000030: 02 00 0f 00 51 51 0f a3 00 00 01 00 00 00 00 00

Pkt# 3 mm/dd/yy 10:20:28.462 CSMACD 60 Rx
00000000: 00 00 a2 00 93 c5 00 00 a2 00 93 c5 81 02 01 01
00000010: 00 00 00 00 30 5b 00 00 00 00 00 00 00 00 00 00
00000020: a9 4b 16 aa e9 1d 00 00 00 00 a8 c0 00 00 00 00
00000030: 14 00 02 00 0f 00 b6 05 5a 51 0f 00 00 00 00 00
```

Example 2

Enter the following command to display all packets starting with the second packet in the Packet Capture file:

pktdump 102101 -s2

```
Pkt#   2 mm/dd/yy 10:20:28.196 CSMACD 60 Rx
00000000: 00 00 a2 03 c1 66 00 00 a2 03 c1 66 81 02 01 01
00000010: 00 00 00 00 00 00 1f 80 00 00 00 a3 00 00 0c 00 00
00000020: 00 00 80 00 00 00 00 a3 00 00 0c 80 07 00 00 14 00
00000030: 02 00 0f 00 51 51 0f a3 00 00 01 00 00 00 00 00

Pkt#   3 mm/dd/yy 10:20:28.462 CSMACD 60 Rx
00000000: 00 00 a2 00 93 c5 00 00 a2 00 93 c5 81 02 01 01
00000010: 00 00 00 00 30 5b 00 00 00 00 00 00 00 00 00 00
00000020: a9 4b 16 aa e9 1d 00 00 00 00 a8 c0 00 00 00 00
00000030: 14 00 02 00 0f 00 b6 05 5a 51 0f 00 00 00 00 00
```

Example 3

Enter the following command to display only the first packet in the Packet Capture file:

pktdump 102101 -c1

```
Pkt#   1 mm/dd/yy 10:20:26.430 CSMACD 60 Rx
00000000: 01 80 c2 00 00 00 00 00 a3 00 00 0c 00 26 42 42
00000010: 03 00 00 00 00 00 80 00 00 00 a3 00 00 0c 00 00
00000020: 00 00 80 00 00 00 00 a3 00 00 0c 80 07 00 00 14 00
00000030: 02 00 0f 00 3f 09 ef df 00 00 01 00 00 00 00 00
```


Example 4

Enter the following command to display only the second packet in the Packet Capture file:

pkt dump 102101 -s2 -c1

```
Pkt#    2 mm/dd/yy 10:20:28.196 CSMACD 60 Rx
00000000: 00 00 a2 03 c1 66 00 00 a2 03 c1 66 81 02 01 01
00000010: 00 00 00 00 00 00 1f 80 00 00 00 a3 00 00 0c 00 00
00000020: 00 00 80 00 00 00 a3 00 00 0c 80 07 00 00 14 00
00000030: 02 00 0f 00 51 51 0f a3 00 00 01 00 00 00 00 00
```

Deleting a Packet Capture Instance

You may want to delete all MIB information about a Packet Capture instance if you no longer intend to use it and you want to free the memory for other purposes. To delete an instance, enter the following command:

set wfPktCaptureEntry.1.<line_no.> 2;commit

1 represents the wfPktCaptureDelete attribute.

<line_no.> is the number displayed after you issued the **get** command in “[Creating an Instance of Packet Capture](#).” To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

2 represents the numeric code for “delete.”

Example

Enter the following command to delete the Packet Capture instance identified by line number 202101:

set wfPktCaptureEntry.1.202101 2;commit

Using Optional Features

The following sections describe how to use optional Packet Capture features:

- [“Configuring the Direction of the Packets to Be Copied”](#)
- [“Configuring a Termination Trigger”](#)
- [“Assigning Filters”](#)



Note: If Packet Capture is running and you change the configuration, the change will not affect Packet Capture until you stop and restart it.

Configuring the Direction of the Packets to Be Copied

This section describes how to change the direction of the packets to be copied. By default, Packet Capture copies only incoming packets.

Enter the following command to change the direction of the packets that Packet Capture copies:

set wfPktCaptureEntry.10.<line_no.> <value>;commit

10 represents the wfPktCaptureDirection attribute.

<line_no.> is the number displayed after you issued the **get** command in [“Creating an Instance of Packet Capture.”](#) To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

<value> is one of the following:

- 1 -- Packet Capture will copy only incoming packets.
- 2 -- Packet Capture will copy only outgoing packets.
- 3 -- Packet Capture will copy both incoming and outgoing packets.

Example

Enter the following command to configure Packet Capture to copy both incoming and outgoing packets associated with line number 102101:

set wfPktCaptureEntry.10.102101 3;commit

Configuring a Termination Trigger

By default, Packet Capture terminates only when you issue the command to terminate it. You can change this default so that Packet Capture terminates when either of the following occurs:

- The Packet Capture file is full.
- It matches a portion of an incoming or outgoing packet to a hexadecimal number or character string that you specify.

You can issue a command to terminate Packet Capture even if you configure it to terminate on its own.

If you want Packet Capture to terminate itself and

- You configured Packet Capture to copy incoming packets, enter the following command:

set wfPktCaptureEntry.12.<line_no.> <value>;commit

12 represents the wfPktCaptureRxTrigger attribute.

- You configured Packet Capture to copy outgoing packets, enter the following command:

set wfPktCaptureEntry.13.<line_no.> <value>;commit

13 represents the wfPktCaptureTxTrigger attribute.

Enter both commands if you want to change the trigger settings for both incoming and outgoing packets.

<line_no.> is the number displayed after you issued the **get** command in “[Creating an Instance of Packet Capture](#).” To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

<value> is one of the following:

- 1 -- Packet Capture terminates when the Packet Capture file is full. If the setting is not 1 and the file is full, Packet Capture overwrites the oldest packets in the file.



Caution: If you configure Packet Capture to copy both incoming and outgoing packets, it copies them to a single file. Therefore, if you choose both packet directions, and set one of these parameters (Receive Trigger or Transmit Trigger) to 1, you must set the other parameter to 1. If you fail to do this, Packet Capture may overwrite the oldest packets, regardless of whether an interface received or transmitted them.

- 2 -- Packet Capture terminates when data matches the value of the Filter 1 Match parameter for the packet direction queried.
- 3 -- Packet Capture terminates when data matches the value of the Filter 2 Match parameter for the packet direction queried.
- 4 -- Packet Capture runs until terminated manually. This is the default setting.

Example

Enter the following command if you configured the Packet Capture instance associated with logical line 102101 to copy only incoming packets, and you want it to terminate itself when it matches packet data to the Filter 2 Match set parameters:

wfPktCaptureEntry.12.102101 3;commit

Assigning Filters

Read this section if you want to specify a string of alphanumeric characters to compare with the packet data.

When Packet Capture matches packet data to the string, it either copies the packet to the Packet Capture file or it terminates without copying the packet. Packet Capture supports two filters for incoming packets and two filters for outgoing packets.

The Packet Capture filter names are as follows:

- Receive Filter 1 matches incoming packet data to a string you specify.
- Receive Filter 2 matches incoming packet data to a second string you specify.
- Transmit Filter 1 matches outgoing packet data to a string you specify.
- Transmit Filter 2 matches outgoing packet data to a second string you specify.

Each filter has its own set of parameters. They are as follows:

- Type

Determines whether Packet Capture terminates when it finds a match, copies a packet when it matches it to the string, or copies every packet on a circuit.

- Match

The hexadecimal number or string of characters that Packet Capture uses to compare to the data in a packet.

- Reference, Offset, and Size

The data in the packet to compare with the string. Reference identifies the field of the packet. Offset determines the number of bytes after the Reference with which to begin the comparison. Size determines the number of bytes to compare to the string.

Packet Capture also supports one Group parameter for each packet direction. The Group parameter allows you to specify whether the packet must match both Filter 1 and Filter 2 in order for Packet Capture to copy it. Refer to the following sections to set the parameters for each filter.



Note: To avoid confusion, configure all of the parameter settings for one filter before going to the next. For example, configure all of the Receive Filter 1 parameters before configuring the Receive Filter 2 parameters.

Setting the Filter Response to a Match

Enter the following Technician Interface command to set the response to the filter:

set wfPktCaptureEntry.<attribute_no>.<line_no> <value>;commit

<attribute_no> is one of the following:

- **14** for Receive Filter 1
Represents the wfPktCaptureRxFltr1Type attribute
- **24** for Receive Filter 2
Represents the wfPktCaptureRxFltr2Type attribute
- **19** for Transmit Filter 1
Represents the wfPktCaptureTxFltr1Type attribute
- **30** for Transmit Filter 2
Represents the wfPktCaptureTxFltr2Type attribute

<line_no> is the number displayed after you issued the **get** command in “[Creating an Instance of Packet Capture](#).” To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

<value> is one of the following:

- 1 -- Packet Capture will copy only the packets containing the data that matches the string.
- 2 -- Packet Capture will terminate when it matches data in a packet to the string. Packet Capture will not copy the packet containing the match.
- 3 -- Packet Capture will copy every packet on a circuit, regardless of its contents. If you use this setting, Packet Capture does not use the remaining parameter settings for the associated filter.



Note: You can configure a filter as a capture type (1) or a trigger type (2), but not both. If you configure two receive filters, one a capture filter and the other a trigger filter, make Filter 2 the trigger filter.

Specifying the String to Compare with the Packet Data

Enter the following Technician Interface command to create a string of characters to compare with the packet:

set wfPktCaptureEntry.<attribute_no.>.<line_no.> <value>;commit

<attribute_no.> is one of the following:

- **18** for Receive Filter 1
Represents the wfPktCaptureRxFltr1Match attribute
- **28** for Receive Filter 2
Represents the wfPktCaptureRxFltr2Match attribute
- **23** for Transmit Filter 1
Represents the wfPktCaptureTxFltr1Match attribute
- **34** for Transmit Filter 2
Represents the wfPktCaptureTxFltr2Match attribute

<line_no.> is the number displayed after you issued the **get** command in “[Creating an Instance of Packet Capture](#).” To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

<value> is any hexadecimal number or character string of up to 16 characters.

Specifying the Data to Compare with the String

Refer to the following sections to specify the data in the packet to compare with the string:

- “[Specifying the Reference](#)”
- “[Specifying the Offset](#)”
- “[Specifying the Number of Bytes](#)”

Specifying the Reference

Enter the following Technician Interface command to specify the Reference, which is the field in the packet:

set wfPktCaptureEntry.<attribute_no.>.<line_no.> <value>;commit

<attribute_no.> is one of the following:

- **16** for Receive Filter 1
Represents the wfPktCaptureRxFltr1Ref attribute
- **26** for Receive Filter 2
Represents the wfPktCaptureRxFltr2Ref attribute
- **21** for Transmit Filter 1
Represents the wfPktCaptureTxFltr1Ref attribute
- **32** for Transmit Filter 2
Represents the wfPktCaptureTxFltr2Ref attribute

<line_no.> is the number displayed after you issued the **get** command in “[Creating an Instance of Packet Capture](#).” To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

<value> is one of the following:

- **1** for the first byte of the packet
Specify 1 if you want the copied portion of the packet to contain MAC address information.
- **2** for data link
- **3** for multicast
Specify 3 if you want to use a special filter to make sure the rightmost bit of a byte is a 1.
To specify a multicast bit for Ethernet, specify 3. Then, set the offset to 0.
To specify a source routing bit for token ring, specify 3. Then, set the offset to 6.

Specifying the Offset

Enter the following Technician Interface command to specify the number of bytes after the Reference with which to begin the comparison:

set wfPktCaptureEntry.<attribute_no.>.<line_no.> <value>;commit

<attribute_no.> is one of the following:

- **15** for Receive Filter 1
Represents the wfPktCaptureRxFltr1Offset attribute
- **25** for Receive Filter 2
Represents the wfPktCaptureRxFltr2Offset attribute
- **20** for Transmit Filter 1
Represents the wfPktCaptureTxFltr1Offset attribute
- **31** for Transmit Filter 2
Represents the wfPktCaptureTxFltr2Offset attribute

<line_no.> is the number displayed after you issued the **get** command in “[Creating an Instance of Packet Capture](#).” To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

<value> is any number up to the number of bytes in the packet. For detailed instructions, refer to the media you are filtering in “[Media-Specific Instructions and Examples](#)” on [page B-51](#).

Specifying the Number of Bytes

Enter the following Technician Interface command to specify the number of bytes to compare with the string:

set wfPktCaptureEntry.<attribute_no.>.<line_no.> <value>;commit

<attribute_no.> is one of the following:

- **17** for Receive Filter 1
Represents the wfPktCaptureRxFltr1Size attribute
- **27** for Receive Filter 2
Represents the wfPktCaptureRxFltr2Size attribute

- **22** for Transmit Filter 1
Represents the wfPktCaptureTxFltr1Size attribute
- **33** for Transmit Filter 2
Represents the wfPktCaptureTxFltr2Size attribute

<line_no.> is the number displayed after you issued the **get** command in “[Creating an Instance of Packet Capture](#).” To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

<value> is the number of characters in the Match parameter setting. It cannot exceed 16.

Selecting the Number of Filters That Must Match

Read this section if you completed both of the following tasks:

- You configured both filters associated with a packet direction.
- You set the Type parameter for both filters to 1 to copy only packets that match the string.

Enter the following command to specify whether the packet must match both Filter 1 and Filter 2 in order for Packet Capture to copy it:

set wfPktCaptureEntry.<attribute_no.>.<line_no.> <value>;commit

<attribute_no.> is one of the following:

- **29** for Receive Filter 1 and Receive Filter 2
Represents the wfPktCaptureRxFltr2Group attribute
- **35** for Transmit Filter 1 and Transmit Filter 2
Represents the wfPktCaptureTxFltr2Group attribute

<line_no.> is the number displayed after you issued the **get** command in “[Creating an Instance of Packet Capture](#).” To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

<value> is one of the following:

- 1 -- Packet Capture will copy a packet if it matches either Filter 1 or Filter 2.
- 2 -- Packet Capture will copy a packet only if it matches both Filter 1 and Filter 2.



Note: Packet Capture uses this parameter only if you configure both capture filters associated with a single direction.

Configuration Examples

This section shows examples of Packet Capture configurations. The circuit is on a CSMA/CD interface. The line number is 102101.

Example 1

This example sets the following configuration:

- 1024 bytes of memory reserved for Packet Capture
- 64 bytes of each packet to be saved
- Incoming and outgoing packets to be saved
- No filters and no triggers

The instructions are as follows:

1. Reserve 1024 bytes of memory:

set wfPktCaptureEntry.8.102101 1

8 represents the wfPktCaptureBufSize attribute.

2. Save 64 bytes of each packet:

set wfPktCaptureEntry.9.102101 2

9 represents the wfPktCapturePktSize attribute.

3. Save incoming and outgoing packets:

set wfPktCaptureEntry.10.102101 3;commit

10 represents the wfPktCaptureDirection attribute.

Example 2

This example starts and stops Packet Capture. The instructions are as follows:

1. Start Packet Capture:

set wfPktCaptureEntry.5.102101 1;commit

5 represents the wfPktCaptureControl attribute.

2. Stop Packet Capture:

set wfPktCaptureEntry.5.102101 2;commit

Example 3

This example configures a termination trigger for each direction. The instructions are as follows:

1. Set a trigger for incoming packets:

set wfPktCaptureEntry.12.102101 1

12 represents the wfPktCaptureRxTrigger attribute.

2. Set a trigger for outgoing packets:

set wfPktCaptureEntry.13.102101 1;commit

13 represents the wfPktCaptureTxTrigger attribute.

Example 4

This example specifies that Packet Capture copy only incoming packets with a Type field containing the hexadecimal number 0800. The instructions are as follows:

1. Copy only incoming packets that match the Receive Filter 1 Match parameter setting:

set wfPktCaptureEntry.14.102101 1

14 represents the wfPktCaptureRxFltr1Type attribute.

2. Specify the Reference with which to begin the comparison:

set wfPktCaptureEntry.16.102101 1

16 represents the wfPktCaptureRxFltr1Ref attribute.

3. **Specify the number of bytes after the Reference with which to begin the comparison:**

set wfPktCaptureEntry.15.102101 12

15 represents the wfPktCaptureRxFiltr1Offset attribute.

4. **Specify the number of bytes in the packet to compare with the string:**

set wfPktCaptureEntry.17.102101 2

17 represents the wfPktCaptureRxFiltr1Size attribute.

5. **Specify the string as the hexadecimal number 0800:**

set wfPktCaptureEntry.18.102101 0x0800;commit

18 represents the wfPktCaptureRxFiltr1Match attribute.

Example 5

This example specifies that Packet Capture copy only incoming packets with both a Type field value of hexadecimal 0800 and a destination MAC address of ffffffff. It assumes you have already specified the Type field as shown in [Example 4](#). The instructions are as follows:

1. **Copy incoming packets that match the Receive Filter 2 Match parameter setting:**

set wfPktCaptureEntry.24.102101 1

24 represents the wfPktCaptureRxFiltr2Type attribute.

2. **Specify the Reference with which to begin the comparison:**

set wfPktCaptureEntry.26.102101 1

26 represents the wfPktCaptureRxFiltr2Ref attribute.

3. **Specify the number of bytes after the Reference with which to begin the comparison:**

set wfPktCaptureEntry.25.102101 0

25 represents the wfPktCaptureRxFiltr2Offset attribute.

4. **Specify the number of bytes in the packet to compare with the string:**

set wfPktCaptureEntry.27.102101 6

27 represents the wfPktCaptureRxFiltr2Size attribute.

5. Specify the string as the hexadecimal number **ffffffffffff**:
set wfPktCaptureEntry.28.102101 0xffffffffffff
28 represents the wfPktCaptureRxFiltr2Match attribute.
6. Specify that Packet Capture copy a packet only if it matches both the Receive Filter 1 Match and Receive Filter 2 Match parameter settings:
set wfPktCaptureEntry.29.102101 2;commit
29 represents the wfPktCaptureRxFiltr2Group attribute.

Displaying the Current Packet Capture Configuration Settings

Enter the following command to display the current Packet Capture configuration:

get wfPktCaptureEntry.*.<line_no.>

<line_no.> is the number displayed after you issued the **get** command in “[Creating an Instance of Packet Capture](#).” To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

The Technician Interface displays a value for each attribute. Go to the “Reference Guide” section for a description of each attribute and its values.

Example

```
get wfPktCaptureEntry.*.102101
wfPktCaptureEntry.wfPktCaptureDelete.102101 = 1
wfPktCaptureEntry.wfPktCaptureDisable.102101 = 1
wfPktCaptureEntry.wfPktCaptureState.102101 = 1
wfPktCaptureEntry.wfPktCaptureFname.102101 = "PCAP0200"
wfPktCaptureEntry.wfPktCaptureControl.102101 = 1
wfPktCaptureEntry.wfPktCaptureCapture.102101 = 2
wfPktCaptureEntry.wfPktCaptureLineNumber.102101 = 102101
wfPktCaptureEntry.wfPktCaptureBufSize.102101 = 0
wfPktCaptureEntry.wfPktCapturePktSize.102101 = 0
wfPktCaptureEntry.wfPktCaptureDirection.102101 = 1
wfPktCaptureEntry.wfPktCaptureCount.102101 = 0
wfPktCaptureEntry.wfPktCaptureRxTrigger.102101 = 4
wfPktCaptureEntry.wfPktCaptureTxTrigger.102101 = 4
wfPktCaptureEntry.wfPktCaptureRxFiltr1Type.102101 = 3
wfPktCaptureEntry.wfPktCaptureRxFiltr1Offset.102101 = 0
wfPktCaptureEntry.wfPktCaptureRxFiltr1Ref.102101 = 1
wfPktCaptureEntry.wfPktCaptureRxFiltr1Size.102101 = 0
```

```
wfPktCaptureEntry.wfPktCaptureRxFltr1Match.102101 = (nil)
wfPktCaptureEntry.wfPktCaptureTxFltr1Type.102101 = 3
wfPktCaptureEntry.wfPktCaptureTxFltr1Offset.102101 = 0
wfPktCaptureEntry.wfPktCaptureTxFltr1Ref.102101 = 1
wfPktCaptureEntry.wfPktCaptureTxFltr1Size.102101 = 0
wfPktCaptureEntry.wfPktCaptureTxFltr1Match.102101 = (nil)
wfPktCaptureEntry.wfPktCaptureRxFltr2Type.102101 = 3
wfPktCaptureEntry.wfPktCaptureRxFltr2Offset.102101 = 0
wfPktCaptureEntry.wfPktCaptureRxFltr2Ref.102101 = 1
wfPktCaptureEntry.wfPktCaptureRxFltr2Size.102101 = 0
wfPktCaptureEntry.wfPktCaptureRxFltr2Match.102101 = (nil)
wfPktCaptureEntry.wfPktCaptureRxFltr2Group.102101 = 1
wfPktCaptureEntry.wfPktCaptureTxFltr2Type.102101 = 3
wfPktCaptureEntry.wfPktCaptureTxFltr2Offset.102101 = 0
wfPktCaptureEntry.wfPktCaptureTxFltr2Ref.102101 = 1
wfPktCaptureEntry.wfPktCaptureTxFltr2Size.102101 = 0
wfPktCaptureEntry.wfPktCaptureTxFltr2Match.102101 = (nil)
wfPktCaptureEntry.wfPktCaptureTxFltr2Group.102101 = 1
```

Displaying Event Messages Issued by Packet Capture

Enter the following Technician Interface command to display the Packet Capture event messages:

log -fftwid -ePCAP

See *Event Messages for Routers* for information about the events.

Using a Sun Workstation or DOS PC to Display Packets

This section covers the following topics:

- [“Getting the Name of the Packet Capture File”](#)
- [“Using FTP to Transfer the File”](#)
- [“Using TFTP to Transfer the File”](#)
- [“Using XMODEM to Transfer the File”](#)
- [“Displaying the File with Packet Dump”](#)

Getting the Name of the Packet Capture File

To get a Packet Capture file stored in the router's memory, you must know its name. Enter the following command to get the file name:

get wfPktCaptureEntry.4.<line_no.>

<line_no.> is the number displayed after you issued the **get** command in "[Creating an Instance of Packet Capture](#)." To list the current line numbers associated with Packet Capture, enter the command **list instances wfPktCaptureEntry**.

4 represents the wfPktCaptureFname attribute.

The file name is formatted as follows:

PCAP<ssnn>

ss is the slot number.

nn is a number from 00 to 99.

Example

Enter the following command to display the name of the captured packets associated with Line No. 102101:

get wfPktCaptureEntry.4.102101

Using FTP to Transfer the File

When you use FTP to get a Packet Capture file, the FTP software transfers it from the processor's memory instead of from the media.

The procedure for using FTP to transfer a copy of a file to a Sun workstation or PC depends on the implementation of FTP on that system. The following instructions apply to Sun workstations.

If you are using a PC and need instructions for using FTP, refer to the documentation for the TCP/IP stack installed on the PC.

Enter the following commands at the command-line interface of the Sun workstation:

1. **Issue the following command to start FTP:**

FTP

2. **Issue the following command to establish an FTP connection with the router:**

open <IP_address>

<IP_address> is the IP address of the router.

Example

connect 1.1.1.1

3. **Enter the following command to specify that the file to be transferred is binary:**

mode binary

4. **Enter the following command to retrieve a copy of the file:**

get <filename>

<filename> is the name displayed after you issued the **get** command in [“Getting the Name of the Packet Capture File.”](#)

Example

get pcap0400

5. **Enter the following command to terminate FTP:**

quit

Using TFTP to Transfer the File

When you use TFTP to get a Packet Capture file, the TFTP software transfers it from the processor’s memory instead of from the media.

The procedure for using TFTP to transfer a copy of a file to a Sun workstation or PC depends on the implementation of TFTP on that system. The following instructions apply to Sun workstations.

If you are using a PC and need instructions for using TFTP, refer to the documentation for the TCP/IP stack installed on the PC.

Enter the following commands at the command-line interface of the Sun workstation:

1. **Issue the following command to start TFTP:**

tftp

2. **Issue the following command to establish a TFTP connection with the router:**

connect <IP_address>

<IP_address> is the IP address of the router.

Example

connect 1.1.1.1

3. **Enter the following command to specify that the file to be transferred is binary:**

mode binary

4. **Enter the following command to retrieve a copy of the file:**

get <filename>

<filename> is the name displayed after you issued the **get** command in [“Getting the Name of the Packet Capture File.”](#)

Example

get pcap0400

5. **Enter the following command to terminate TFTP:**

quit

Using XMODEM to Transfer the File

Enter the following Technician Interface command to transfer a copy of the Packet Capture file from the router processor's memory:

xmodem sb *<filename>*

<filename> is the name displayed after you issued the **get** command in “[Getting the Name of the Packet Capture File](#).”



Note: Bay Networks supports only single-file mode for the XMODEM protocol. Bay Networks does not support the YMODEM protocol.

Displaying the File with Packet Dump

You can use the Packet Dump utility to display a Packet Capture file that you retrieved from the router.

The Site Manager installation software installs the Packet Dump utility on the following platforms:

- On DOS PCs, in the *\wf* directory. The file name is *pktdump.dos*.
- On Sun workstations, in the */usr/wf/bin* directory. The file name is *pktdump.spc*. This version runs only on SunOS.

These utilities are also available in the */perm/pkt_dump* directory on the Bay Networks FTP file server. See Chapter 8 for file-transfer instructions.

Access the directory and enter the following command at the DOS or UNIX command line:

pktdump *<filename>*

<filename> is the name of the Packet Capture file you retrieved from the router.

Packet Dump shows the same information about each packet as the Technician Interface, but it does not provide options for specifying the packet by number or quantity. See “[Using the Technician Interface to Display a Packet Capture File](#)” earlier in this appendix for a description of the fields; [Example 1](#) in that section provides a sample display.

Converting a Packet Capture File to Network General Sniffer Format

You can use the Packet Convert utility to convert a Packet Capture file that you retrieved from the router to Network General Sniffer format. This format allows the Sniffer to use the high level of decoding available to decode the captured packets.

The Site Manager installation software installs the Packet Convert utility on the following platforms:

- On DOS PCs, in the \wf directory. The file name is *pktconv.dos*.
- On Sun workstations, in the /usr/wf/bin directory. The file name is *pktconv.spc*. This version runs only on SunOS.

These utilities are also available in the /perm/pkt_convert directory on the Bay Networks FTP file server. See Chapter 8 for file-transfer instructions.

The Network General Sniffer reads MCT1 Packet Capture files as synchronous files.

You can convert HSSI packets only if the protocol is standard synchronous, such as PPP. You cannot convert packets if the protocol is HPTP.

Packet Convert does not support the bisynchronous protocol.



Note: Before you can capture packets, you must set the size of the packets to a value that the Sniffer supports. See “[Specifying the Number of Bytes in Each Packet to Copy](#)” on [page B-12](#) for instructions.

Convert a Packet Capture file as follows:

- 1. Retrieve a copy of the file from the router.**

See the following sections for instructions:

- “[Getting the Name of the Packet Capture File](#)” ([B-32](#))
- “[Using FTP to Transfer the File](#)” ([B-32](#)), “[Using TFTP to Transfer the File](#)” ([B-33](#)), or “[Using XMODEM to Transfer the File](#)” ([B-35](#))

- 2. Make sure the file name does not have an extension and does not exceed 8 characters.**

3. Access the directory containing the **Packet Convert** utility.
4. Enter the following command to convert the file:

pktconv <filename>

Packet Capture creates a new file that you can copy to a DOS-formatted diskette and insert in the Sniffer. The name of the file begins with the Packet Capture file name and ends with the extension the Sniffer requires.

Examples

- For a CSMA/CD Packet Capture file named *PCAP0400*, enter the following:

pktconv pcap0400

Packet Convert creates a Sniffer file named *PCAP0400.ENC*.

- For a token ring Packet Capture file named *PCAP0300*, enter the following:

pktconv pcap0300

Packet Convert creates a Sniffer file named *PCAP0300.TRC*.

- For a synchronous Packet Capture file named *PCAP0200*, enter the following:

pktconv pcap0200

Packet Convert creates a Sniffer file named *PCAP0200.SYC*.

- For a FDDI Packet Capture file named *PCAP0500*, enter the following:

pktconv pcap0500

Packet Convert creates a Sniffer file named *PCAP0500.FDC*.



Note: If you use PPP, the file will convert, but you must use the Sniffer Protocol Forcing option in order to decode the packets.

Reference Guide to Packet Capture

This reference guide contains the following sections:

- [“Displaying the Packet Capture Attribute Names and Numbers”](#)

- [“Packet Capture Parameter Descriptions”](#)
- [“Media-Specific Instructions and Examples”](#)
- [“Interpreting a Packet Capture Instance Number”](#)

Displaying the Packet Capture Attribute Names and Numbers

Enter the following command to display the attributes of the Packet Capture (wfPktCaptureEntry) object and their associated numeric identifiers:

list wfPktCaptureEntry



Note: Do not confuse the numeric identifier next to an attribute name with the value of that attribute. The numeric identifier is an alternative way to identify an attribute when issuing a **get** command. To get the values of the Packet Capture attributes, see [“Displaying the Current Packet Capture Configuration Settings”](#) on [page B-30](#).

Example

```
list wfPktCaptureEntry
wfPktCaptureDelete = 1
wfPktCaptureDisable = 2
wfPktCaptureState = 3
wfPktCaptureFname = 4
wfPktCaptureControl = 5
wfPktCaptureCapture = 6
wfPktCaptureLineNumber = 7
wfPktCaptureBufSize = 8
wfPktCapturePktSize = 9
wfPktCaptureDirection = 10
wfPktCaptureCount = 11
wfPktCaptureRxTrigger = 12
wfPktCaptureTxTrigger = 13
wfPktCaptureRxFltr1Type = 14
wfPktCaptureRxFltr1Offset = 15
wfPktCaptureRxFltr1Ref = 16
wfPktCaptureRxFltr1Size = 17
wfPktCaptureRxFltr1Match = 18
wfPktCaptureTxFltr1Type = 19
wfPktCaptureTxFltr1Offset = 20
wfPktCaptureTxFltr1Ref = 21
wfPktCaptureTxFltr1Size = 22
wfPktCaptureTxFltr1Match = 23
wfPktCaptureRxFltr2Type = 24
```

```
wfPktCaptureRxFltr2Offset = 25
wfPktCaptureRxFltr2Ref = 26
wfPktCaptureRxFltr2Size = 27
wfPktCaptureRxFltr2Match = 28
wfPktCaptureRxFltr2Group = 29
wfPktCaptureTxFltr2Type = 30
wfPktCaptureTxFltr2Offset = 31
wfPktCaptureTxFltr2Ref = 32
wfPktCaptureTxFltr2Size = 33
wfPktCaptureTxFltr2Match = 34
wfPktCaptureTxFltr2Group = 35
```

Packet Capture Parameter Descriptions

The following sections describe each parameter, its equivalent number, and its valid values:

- [“Basic Parameters”](#)
- [“Trigger Parameters”](#)
- [“Filter Parameters”](#)



Note: Packet Capture reads attribute values only when it starts. To make Packet Capture respond to a change to an attribute value, stop and then restart it.

If you configure an invalid value for an attribute, an error message appears in the log.

Basic Parameters

The basic parameters are common to all Packet Capture configurations. The basic parameters described in this section are as follows:

- [Delete](#)
- [Disable](#)
- [State](#)
- [Filename](#)
- [Control](#)
- [Capture](#)
- [Line Number](#)
- [Buffer Size](#)
- [Packet Size](#)
- [Direction](#)
- [Count](#)

Parameter: Delete

Attribute Name: wfPktCaptureDelete

Attribute Number: 1

Default: 1 (Create)

Options: 1 (Create) | 2 (Delete)

Function: The Create value reserves a memory location for a Packet Capture instance; Delete removes it.

Instructions: Specify the value 1 to create the instance. Specify the value 2 to delete the instance if you do not plan to use it again; this will free the resources that Packet Capture uses.

MIB Object ID: 1.3.6.1.4.1.18.3.4.21.1.1.1

Parameter: Disable

Attribute Name: wfPktCaptureDisable
Attribute Number: 2
Default: 1 (Enable)
Options: 1 (Enable) | 2 (Disable)
Function: Controls the state of the Packet Capture instance.
Instructions: Disabling an instance frees all resources allocated for the instance. If you previously allocated a file stored in buffer memory, disabling the instance is an easy way to free the file stored in buffer memory and to keep the MIB instance for future captures.
MIB Object ID: 1.3.6.1.4.1.18.3.4.21.1.1.2

Parameter: State

Attribute Name: wfPktCaptureState
Attribute Number: 3
Default: 1 (Up)
Options: 1 (Up) | 2 (Down) | 3 (Init) | 4 (Not present)
Up: An interface has registered and is enabled.
Down: An interface has registered, but has been disabled.
Init: Packet Capture is loaded on the slot, but there is no interface registered for this instance.
Not present: Packet Capture is not loaded on the slot with which this instance is connected.
Function: Indicates the state of the Packet Capture subsystem.
MIB Object ID: 1.3.6.1.4.1.18.3.4.21.1.1.3

Parameter: Filename

Attribute Name: wfPktCaptureFname
 Attribute Number: 4
 Default: Set by Packet Capture code
 Options: PCAP<*ssnn*>
ss is the slot number and *nn* is a number from 00 to 99.
 Function: Packet Capture sets this attribute, which contains the file name that you can use to retrieve the file stored in buffer memory for this instance.
 MIB Object ID: 1.3.6.1.4.1.18.3.4.21.1.1.4

Parameter: Control

Attribute Name: wfPktCaptureControl
 Attribute Number: 5
 Default: 2 (Stop)
 Options: 1 (Start) | 2 (Stop)
 Start: Starts copying to a file
 Stop: Terminates copying to a file
 Function: Manually starts and stops a capture for this instance. You must stop Packet Capture before you can display the packets.
 MIB Object ID: 1.3.6.1.4.1.18.3.4.21.1.1.5

Parameter: Capture

Attribute Name: wfPktCaptureCapture
 Attribute Number: 6
 Default: 2 (Stop)
 Options: 1 (Start) | 2 (Stop)
 Function: Indicates whether Packet Capture has started or stopped.
 MIB Object ID: 1.3.6.1.4.1.18.3.4.21.1.1.6

Parameter: Line Number

Attribute Name: wfPktCaptureLineNumber
Attribute Number: 7
Default: Set by Packet Capture code
Options: Based on the encoded value
Function: Uniquely identifies a circuit.
MIB Object ID: 1.3.6.1.4.1.18.3.4.21.1.1.7

Parameter: Buffer Size

Attribute Name: wfPktCaptureBufSize
Attribute Number: 8
Default: None
Options: 1 (allocates 1024 bytes) | 2 (allocates 2048 bytes) | Up to the available contiguous memory divided by 1024
Function: Sets the size of the file stored in buffer memory, in 1024-byte increments. The upper limit is the maximum number of contiguous bytes of memory available on the slot. You can determine the maximum number of contiguous bytes by entering the following command:
get wfKernelEntry.6.<slot no.>
6 represents the wfKernelMemoryMaxSegFree attribute.
Instructions: If the allocation of the buffer leaves less than 200 KB of memory, a warning appears in the log. The operating system may need to allocate and free memory. If the memory needed is not available, an error occurs. If errors occur after you start Packet Capture, stop it and allocate a smaller buffer size.
MIB Object ID: 1.3.6.1.4.1.18.3.4.21.1.1.8

Parameter: Packet Size

Attribute Name: wfPktCapturePktSize
 Attribute Number: 9
 Default: None
 Range: 1 (32 bytes saved) | 2 (64 bytes saved) | Up to 144 (4608 bytes saved)
 Function: Sets the number of bytes, in 32-byte increments, to be saved from a packet.
 MIB Object ID: 1.3.6.1.4.1.18.3.4.21.1.1.9

Parameter: Direction

Attribute Name: wfPktCaptureDirection
 Attribute Number: 10
 Default: 1 (Receive)
 Options: 1 (Receive) | 2 (Transmit) | 3 (Both)
 Function: Sets the direction of Packet Capture: copy received (incoming) packets, transmitted (outgoing) packets, or both.
 MIB Object ID: 1.3.6.1.4.1.18.3.4.21.1.1.10

Parameter: Count

Attribute Name: wfPktCaptureCount
 Attribute Number: 11
 Default: Set by Packet Capture code
 Options: Based on size of buffer and number of bytes saved
 Function: Indicates the number of packets copied to the Packet Capture file.
 Instructions: If you use the default setting of the Trigger parameter and the capture buffer wraps, the count stops when it reaches a maximum value.
 MIB Object ID: 1.3.6.1.4.1.18.3.4.21.1.1.11

Trigger Parameters

You use triggers to stop copying packets when an event occurs. The trigger parameters consist of a receive trigger and a transmit trigger. Each trigger stops Packet Capture, regardless of whether it is copying packets received, transmitted, or both. A description of the trigger parameters follows.

Parameter: Trigger

Packet Capture supports two trigger parameters. The MIB information is as follows:

Packet Direction	Attribute Name	Attribute No.	MIB Object ID
Incoming	wfPktCaptureRxTrigger	12	1.3.6.1.4.1.18.3.4.21.1.1.12
Outgoing	wfPktCaptureTxTrigger	13	1.3.6.1.4.1.18.3.4.21.1.1.13

Default: 4 (Not used)

Options: 1 (Buffer full) | 2 (Match Filter 1) | 3 (Match Filter 2) | 4 (Not used)

Function: Sets Packet Capture to terminate automatically when the packet data matches a string that you specify or when the Packet Capture file is full.

The receive trigger parameter terminates Packet Capture if you set it to a filter, and the incoming packet data matches a string that you specify.

The transmit trigger parameter terminates Packet Capture if you set it to a filter, and the outgoing packet data matches a string that you specify.

Instructions: If you want Packet Capture to terminate when the Packet Capture file is full, set the receive and transmit triggers to 1. If you select an option other than 1 and the file is full, Packet Capture overwrites the oldest packets in the file.



Caution: If you configure Packet Capture to copy both incoming and outgoing packets, it copies them to a single file. Therefore, if you choose both packet directions, and you set one of these parameters (Receive Trigger or Transmit Trigger) to 1, you must set the other parameter to 1. If you fail to do this, Packet Capture may overwrite the oldest packets, regardless of whether an interface received or transmitted them.

If you want Packet Capture to terminate when it matches data to a string you specify, use one of the following options:

- 2 to terminate when data matches the filter 1 match parameter setting
- 3 to terminate when data matches the filter 2 match parameter setting

If you set the receive trigger parameter to 2 or 3, Packet Capture terminates upon matching data to either filter.

If you do not want Packet Capture to terminate automatically, use the default option (4).

Filter Parameters

The filter parameters described in this section are as follows:

- [Type](#)
- [Offset](#)
- [Reference](#)
- [Size](#)
- [Match](#)
- [Group](#)

Parameter: Type

Packet Capture supports four Type parameters.

Packet Direction	MIB Attribute Name	Filter No.	MIB Object ID	Attribute No.
Incoming	wfPktCaptureRxFltr1Type	1	1.3.6.1.4.1.18.3.4.21.1.1.14	14
Incoming	wfPktCaptureRxFltr2Type	2	1.3.6.1.4.1.18.3.4.21.1.1.24	24
Outgoing	wfPktCaptureTxFltr1Type	1	1.3.6.1.4.1.18.3.4.21.1.1.19	19
Outgoing	wfPktCaptureTxFltr2Type	2	1.3.6.1.4.1.18.3.4.21.1.1.30	30

Default: 3

Options: 1 | 2 | 3

Function: Sets Packet Capture filtering for each filter type.

Instructions: Set to 1 (capture) if you want Packet Capture to copy only the packets containing the data that matches the string.

 Set to 2 (trigger) if you want Packet Capture to terminate when it matches data in a packet to the string. Packet Capture does not copy the packet containing the match.

 Set to 3 if you want Packet Capture to copy every packet on a circuit, regardless of its contents.



Note: You can configure a filter as a capture type or a trigger type, but not both. If you want to configure two receive filters, one a capture filter and the other a trigger filter, configure the trigger filter after the capture filter.

Parameter: Offset

Packet Capture supports four Offset parameters.

Packet Direction	MIB Attribute Name	Filter No.	MIB Object ID	Attribute No.
Incoming	wfPktCaptureRxFiltr1Offset	1	1.3.6.1.4.1.18.3.4.21.1.1.15	15
Incoming	wfPktCaptureRxFiltr2Offset	2	1.3.6.1.4.1.18.3.4.21.1.1.25	25
Outgoing	wfPktCaptureTxFiltr1Offset	1	1.3.6.1.4.1.18.3.4.21.1.1.20	20
Outgoing	wfPktCaptureTxFiltr2Offset	2	1.3.6.1.4.1.18.3.4.21.1.1.31	31

Default: None

Options: Limited to size of buffer

Function: Sets the offset, in bytes, from the reference point to the packet. The byte that the offset points to is the first byte in the packet that will be checked for a match.

Instructions: Refer to the media you are filtering in the section “[Media-Specific Instructions and Examples](#)” on [page B-51](#).

Parameter: Reference

Packet Capture supports four Reference parameters.

Packet Direction	MIB Attribute Name	Filter No.	MIB Object ID	Attribute No.
Incoming	wfPktCaptureRxFltr1Ref	1	1.3.6.1.4.1.18.3.4.21.1.1.16	16
Incoming	wfPktCaptureRxFltr2Ref	2	1.3.6.1.4.1.18.3.4.21.1.1.26	26
Outgoing	wfPktCaptureTxFltr1Ref	1	1.3.6.1.4.1.18.3.4.21.1.1.21	21
Outgoing	wfPktCaptureTxFltr2Ref	2	1.3.6.1.4.1.18.3.4.21.1.1.32	32

Default: 1

Options: 1 | 2 | 3

Function: Indicates the field in the packet to match.

Instructions: Set to one of the following:

- 1 for the first byte of the packet. Specify this value if you want the copied portion of the packet to contain media access control (MAC) information.
- 2 for data link.
- 3 for multicast. Specify this value if you want to use a special filter to make sure the rightmost bit of a byte is 1.

To specify a multicast bit for Ethernet, specify 3. Then, set the offset to 0.

To specify a source routing bit for token ring, specify 3. Then, set the offset to 6.

Parameter: Size

Packet Capture supports four Size parameters.

Packet Direction	MIB Attribute Name	Filter No.	MIB Object ID	Attribute No.
Incoming	wfPktCaptureRxFltr1Size	1	1.3.6.1.4.1.18.3.4.21.1.1.17	17
Incoming	wfPktCaptureRxFltr2Size	2	1.3.6.1.4.1.18.3.4.21.1.1.27	27
Outgoing	wfPktCaptureTxFltr1Size	1	1.3.6.1.4.1.18.3.4.21.1.1.22	22
Outgoing	wfPktCaptureTxFltr2Size	2	1.3.6.1.4.1.18.3.4.21.1.1.33	33

Default: None

Options: Maximum of 16 bytes

Function: Sets the length, in bytes, of the match field.

Instructions: Set the size to equal the number of characters in the Match parameter setting.

Parameter: Match

Packet Capture supports four Match parameters.

Packet Direction	Attribute Name	Filter No.	MIB Object ID	Attribute No.
Incoming	wfPktCaptureRxFltr1Match	1	1.3.6.1.4.1.18.3.4.21.1.1.18	18
Incoming	wfPktCaptureRxFltr2Match	2	1.3.6.1.4.1.18.3.4.21.1.1.28	28
Outgoing	wfPktCaptureTxFltr1Match	1	1.3.6.1.4.1.18.3.4.21.1.1.23	23
Outgoing	wfPktCaptureTxFltr2Match	2	1.3.6.1.4.1.18.3.4.21.1.1.34	34

Default: None

Options: Any hexadecimal number or character string

Function: Sets the hexadecimal number or character string to compare with the packet for a match.

Instructions: Specify any hexadecimal number or character string of up to 16 characters.

Parameter: Group

Packet Capture supports two Group parameters: one for incoming packets and one for outgoing packets.

Packet Direction	MIB Attribute Name	MIB Object ID	Attribute No.
Incoming	wfPktCaptureRxFltr2Group	1.3.6.1.4.1.18.3.4.21.1.1.29	29
Outgoing	wfPktCaptureTxFltr2Group	1.3.6.1.4.1.18.3.4.21.1.1.35	35

Default: 1 (OR)

Options: 1 (OR) | 2 (AND)

Function: Determines whether Packet Capture copies a packet if it matches either filter or both filters. Packet Capture uses this parameter only if you configure both capture filters associated with a single direction.

Instructions: Use one of the following settings for each packet direction:

- 1 if you want Packet Capture to copy a packet if it matches either filter 1 or filter 2
- 2 if you want Packet Capture to copy a packet only if it matches both filter 1 and filter 2

Media-Specific Instructions and Examples

The following sections provide instructions and show examples of packets with different media types. They assume that you set the number of bytes to copy from each packet to 64 by setting the wfPktCapturePktSize (wfPktCaptureEntry.9) to 2. Each example uses the **pktdump** command to show a hexadecimal decoding of a frame or packet.

CSMA/CD

The CSMA/CD (Ethernet) physical medium has a data link filter offset of 14 bytes from the beginning of the MAC header. This places the data link filter point at the first byte after the TYPE/LENGTH field. Outgoing packets may contain less than 60 bytes each because they go to Packet Capture without padding.

An example of a hexadecimal display of a CSMA/CD frame follows.

```
Pkt# 10 mm/dd/yy 10:20:32.670 CSMACD 60 Rx
00000000: 01 80 c2 00 00 00 00 00 a3 00 00 0c 00 26 42 42
00000010: 03 00 00 00 00 00 80 00 00 00 a3 00 00 0c 00 00
00000020: 00 00 80 00 00 00 a3 00 00 0c 80 07 00 00 14 00
00000030: 02 00 0f 00 00 00 00 02 00 00 01 00 00 00 00 00
```

Protocols Supported by Synchronous, T1, E1, and MCT1 Media

The following sections identify the format and filter offsets of the protocols supported by the synchronous, T1, E1, and MCT1 media, and show examples of these packets:

- [“ATM”](#)
- [“Bisynchronous”](#)
- [“Frame Relay”](#)
- [“Frame Relay Switch and SMDS Switch”](#)
- [“LAPB”](#)
- [“Passthru”](#)
- [“Bay Networks Proprietary PPP”](#)
- [“Standard PPP”](#)
- [“SDLC”](#)
- [“SMDS”](#)
- [“X.25”](#)

ATM

The asynchronous transfer mode (ATM) protocol does not have a special data link filter offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works.

An example of a hexadecimal display of an ATM packet follows:

```
Pkt# 20 04/23/98 09:57:29.968 ATM 548 Tx
00000000: 0c 80 00 85 00 4b 02 18 03 cc 45 00 02 14 01 10
00000010: 00 00 01 11 ed c9 64 00 00 01 64 ff ff ff 02 08
00000020: 02 08 02 00 69 c8 02 01 00 00 00 02 00 00 c0 20
00000030: de 00 00 00 00 00 00 00 00 00 00 00 02 00 02
```

Bisynchronous

The bisynchronous (BISYNC) protocol does not have a special data link filter. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works. The captured bisynchronous packets contain a 4-byte prefix that consists of internal information. This prefix is not present in the packets as they appear on the wire. The software uses the prefix to calculate an offset into the packet for filtering.

An example of a hexadecimal display of a bisynchronous packet follows:

```
Pkt#      1 01/01/98 03:17:56.284 BISYNC      9 Tx
00000000: 00 00 07 52 40 40 7f 7f 2d
```

Frame Relay

Frame Relay does not have a special data link filter offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works.

An example of a hexadecimal display of a Frame Relay packet follows:

```
Pkt# 10 04/22/98 08:10:24.706 FR 45 Rx
00000000: 04 01 03 00 80 00 80 c2 00 0e 00 00 00 00 00 80
00000010: 00 00 00 a3 00 00 0c 00 00 00 00 80 00 00 00 a3
00000020: 00 00 0c 80 05 00 00 14 00 02 00 0f 00 9e 00 0e
```

Frame Relay Switch and SMDS Switch

The Frame Relay switch and SMDS switch work the same way as described in the [“Frame Relay”](#) and [“SMDS”](#) sections.

LAPB

The Link Access Procedure-Balanced (LAPB) protocol does not have a special data link filter offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works.

An example of a hexadecimal display of a LAPB packet follows:

```
Pkt# 7 07/20/95 14:22:17.820 LAPB 5 Rx
00000000: 03 64 10 01 81
```

Passthru

The Passthru (PASS) protocol does not have a special data link filter offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works.

An example of a hexadecimal display of a Passthru packet follows:

```
Pkt#    9 04/26/98 09:00:50.730 PASS 24 Tx
00000000: 07 03 00 00 a2 02 c9 b6 00 00 a2 02 c9 b6 81 02
00000010: 01 01 00 00 00 00 00 2a 00 00 00 00 00 00 00 00
```

Standard PPP

Standard point-to-point protocol (PPP) does not have a special data link filter offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works.

An example of a hexadecimal display of a PPP packet follows:

```
Pkt#    9 04/18/98 12:58:45.551 PPP 39 Rx
00000000: ff 03 02 01 00 00 00 00 00 80 00 00 00 a3 00 00
00000010: 0c 00 00 00 00 80 00 00 00 a3 00 00 0c 80 02 00
00000020: 00 14 00 02 00 0f 00 1d 00 00 00 00 00 00 00 00
```

Bay Networks Proprietary PPP

Bay Networks Proprietary PPP has a data link filter offset of 16 bytes from the beginning of the packet. The data link filter is the first byte after the TYPE/LENGTH field.

Packet Capture receives the PPP packets without a reliable address field. This means that the packets marked Tx (for “transmit”) have an accurate address field, but the packets marked Rx (for “receive”) do not have an accurate address field.

An example of a hexadecimal display of a PPP packet follows:

```
Pkt#    9 04/22/98 08:07:52.812 PTP 54 Rx
00000000: 03 03 01 80 c2 00 00 00 00 00 a3 00 00 0c 00 26
00000010: 42 42 03 00 00 00 00 00 80 00 00 00 a3 00 00 0c
00000020: 00 00 00 00 80 00 00 00 a3 00 00 0c 80 01 00 00
00000030: 14 00 02 00 0f 00 6b 0d 00 00 00 00 00 00 00 00
```

SDLC

The Synchronous Data Link Control (SDLC) protocol does not have a special data link filter offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works.

An example of a hexadecimal display of an SDLC packet follows:

```
Pkt# 1 07/20/95 14:45:27.910 SDLC 2 Tx
00000000: d1 bf
```

SMDS

The switched multimegabit data service (SMDS) protocol does not have a special data link filter offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works.

An example of a hexadecimal display of an SMDS packet follows:

```
Pkt# 10 04/22/98 08:09:20.211 SMDS 88 Rx
00000000: 05 03 00 00 00 87 00 4c e1 58 07 97 12 12 ff ff
00000010: c1 58 07 97 54 36 ff ff 05 03 00 00 03 00 01 00
00000020: 00 00 00 00 00 00 00 00 aa aa 03 00 80 c2 00 0e
00000030: 00 00 00 00 00 80 00 00 00 a3 00 00 0c 00 00 00
```

X.25

The X.25 protocol does not have a special data link filter offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works. The X.25 protocol uses the hardware's link layer capabilities, which means that Packet Capture receives only the frame's layer 3 (packet layer) data.

An example of a hexadecimal display of an X.25 packet follows:

```
Pkt# 8 04/26/98 09:00:42.103 X25 47 Rx
00000000: 10 01 e2 00 00 00 00 00 01 00 00 00 00 00 02 00
00000010: 1e aa aa 03 00 00 a2 80 ff 00 00 a2 02 c9 b6 00
00000020: 00 a2 02 c9 b6 81 02 01 01 00 00 00 00 00 38 10
```

Token Ring

The token ring physical medium has a data link filter offset of 14 bytes plus the routing information field (RIF), if one is present. This places the data link filter point at the DSAP (destination service access point) byte. Packet Capture receives only LLC frames from the token ring. It does not receive the access control and frame control bytes at the beginning of each packet. Packet Capture inserts the hexadecimal value 1040 at the beginning of each packet for compatibility and possible future use.

An example of a hexadecimal display of a token ring frame follows:

```
Pkt# 10 04/18/98 12:58:58.885 TOKEN 52 Rx
00000000: 10 40 c0 00 00 00 01 00 00 00 c5 00 00 30 42 42
00000010: 03 00 00 00 00 00 80 00 00 00 a3 00 00 0c 00 00
00000020: 00 00 80 00 00 00 a3 00 00 0c 80 06 00 00 14 00
00000030: 02 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00
```

FDDI

The Fiber Distributed Data Interface (FDDI) physical medium has a data link filter offset of 13 bytes. This places the data link filter point at the DSAP byte. Packet Capture does not receive all frames from the FDDI because the hardware handles certain frames.

An example of a hexadecimal display of a FDDI frame follows:

```
Pkt# 10 04/18/98 12:59:04.017 FDDI 51 Rx
00000000: 50 80 01 43 00 00 00 00 00 c5 00 00 30 42 42 03
00000010: 00 00 00 00 00 80 00 00 00 a3 00 00 0c 00 00 00
00000020: 00 80 00 00 00 a3 00 00 0c 80 08 00 00 14 00 02
00000030: 00 0f 00 b7 00 00 00 00 00 00 00 00 00 00 00 00
```

HSSI

The high-speed serial interface (HSSI) physical medium works exactly the same way as the previously described serial media (see [“Protocols Supported by Synchronous, T1, E1, and MCT1 Media”](#) on [page B-52](#)), except for the HPTP (Standard) protocol.

HPTP has a data link filter offset of 14 bytes from the beginning of the packet. This places the data link filter point at the first byte after the TYPE/LENGTH field. The HPTP packets do not have an address or control field.

An example of a hexadecimal display of a HSSI frame follows:

```
Pkt# 7 04/21/98 09:17:53.957 HPTP 52 Rx
00000000: 01 80 c2 00 00 00 00 00 a3 00 00 0c 00 26 42 42
00000010: 03 00 00 00 00 00 80 00 00 00 a3 00 00 0c 00 00
00000020: 00 00 80 00 00 00 a3 00 00 0c 80 01 00 00 14 00
00000030: 02 00 0f 00 6b 0d 00 00 00 00 00 00 00 00 00 00
```

ISDN

For each of the protocols supported over ISDN, the ISDN B channel works the same way as the previously described serial media (see [“Protocols Supported by Synchronous, T1, E1, and MCT1 Media”](#) on [page B-52](#)).

The ISDN D channel does not have a special data link offset. If you configure a data link filter, set the offset to 0. The data link filter works the same way that the MAC filter works.

An example of a hexadecimal display of an ISDN frame follows:

```
Pkt# 1 11/02/98 16:04:06.151 LAPD 26 Tx
00000000: 00 ad 00 00 08 01 01 05 a1 04 02 88 90 18 01 83
00000010: 70 08 80 32 32 34 30 33 38 37
```

Interpreting a Packet Capture Instance Number

When you create an instance of Packet Capture, you refer to the MIB to get the numeric identifier, called a line number, of the Data Path channel. You then copy the line number when creating the Packet Capture instance. The instructions are provided in [“Creating an Instance of Packet Capture”](#) on [page B-7](#).

Site Manager automatically creates the line numbers when you use it to create a configuration file. A line number is a 10-digit, decimal number that is unique for each Data Path channel in a router.

[Table B-3](#) indicates the structure of a line number or Packet Capture instance number. The top row in the table is for the most significant digit, and the bottom row is for the least significant digit.

Table B-3. Structure of a Line Number

Field	No. of Digits Reserved in the Field	Description
rsvd	1	Reserved and set to zero
chan	2	Line index for devices that use multiple lines per channel (zero for most boards)
type	2	The physical media type, which is one of the following: 1 for CSMA/CD 2 for synchronous 3 for T1 4 for E1 5 for token ring 6 for FDDI 7 for HSSI 9 for MCT1 13 for ISDN D channel 15 for bisynchronous
slot	2	Slot number
mod	1	Module number. On the ASN, the module number is in the range 1 to 4. All other platforms require that you set it to 1.
conn	2	Connector number for the specific medium

Example

The code for a single CSMA/CD interface on slot 2 using XCVR1 is 0000102101. Site Manager removes the leading zeros, assigning a line number of 102101.

Appendix C

Packet Configuration

The **config packet** command enables you to configure the Packet Capture utility using the Technician Interface. For information about the Bay Networks implementation of Packet Capture, see Appendix B.

The **config packet** command has the following subcommand options:

- **config packet line** [*<line_number>*]
- **config packet load** [*<slot>*]
- **config packet unload** [*<slot>*]



Note: As with other script commands, entering ? as an option to **config packet** invokes Technician Interface online Help for that command.

This appendix describes how to configure the Packet Capture utility using the **config packet** command.

Topic	Page
Using the Line Subcommand	C-2
Using the Load Subcommand	C-5
Using the Unload Subcommand	C-5

Using the Line Subcommand

config packet line [*<line_number>*] configures packet capturing on the specified line.

<line_number> specifies the number of the physical line. You can enter the line number on the command line or have the script prompt you for it.

The **config packet line** command prompts you for the media type, slot number, and connector number, so you should gather this information before you begin. After you enter this information, the script displays available memory and the maximum packet save size.

As it runs, the script displays the current values of the following items and asks you to either press [Return] to confirm or enter a new value:

- Capture buffer size
- Packet save size
- Capture direction options: receive, transmit, or both
- Receive trigger options (when to stop capturing packets): when buffer is full, when filter 1 is matched, when filter 2 is matched, or no filter
- Transmit trigger options (when to stop capturing packets): when buffer is full, when filter 1 is matched, when filter 2 is matched, or no filter
- Receive filter configuration: Type and Reference options
- Transmit filter configuration: Type and Reference options

For information about all these options, see Appendix B.

The following is a sample display of the **config packet line** command:

```
config packet line
Performing mount check...

Packet Capture Line Configuration
-----
Media Types
-----
1: Ethernet
2: Synchronous or ISDN B Channel
3: T1
4: E1
```

5: Token Ring

6: FDDI

7: HSSI

9: MCT1

13: ISDN D Channel

Enter media type by number: 1

Enter slot number: 5

Enter connector number: 3

The calculated Linenumber is 105103

Please record it for use with other packet commands.

Current available memory in 1Kbyte blocks is 2609

Do not leave less than 200 blocks available unless necessary

Current value for Capture Buffer size in 1Kbyte blocks is 0

Press return for current value or enter new value: 1

Maximum Packet Save size in 32 Byte blocks is 32

Current value for Packet Save size in 32 Byte blocks is 0

Press return for current value or enter new value: 2

Capture Direction Options

1: Receive

2: Transmit

3: Receive and Transmit

Current value for Capture Direction is 1

Press return for current value or enter new value: 3

Receive Trigger Options

1: Stop Capture when Capture Buffer is Full

2: Stop Capture when Receive Filter One is Matched

3: Stop Capture when Receive Filter Two is Matched

4: No Receive Trigger

Current value for Receive Trigger is 4

Press return for current value or enter new value: 4

Transmit Trigger Options

- 1: Stop Capture when Capture Buffer is Full
- 2: Stop Capture when Transmit Filter One is Matched
- 3: Stop Capture when Transmit Filter Two is Matched
- 4: No Transmit Trigger

Current value for Transmit Trigger is 4

Press return for current value or enter new value: 4

Packet Capture Receive Capture Filter Configuration

Receive Filter One Type Options

1: Capture

3: Not Used

Current value for Receive Filter One Type is 3

Press return for current value or enter new value: 1

Current value for Receive Filter One Offset is 0

Press return for current value or enter new value:

Receive Filter One Reference Options

1: Mac

2: Data Link

3: Multicast

Current value for Receive Filter One Reference is 1

Press return for current value or enter new value:

Current value for Receive Filter One Size is 0

Press return for current value or enter new value: 6

Current value for Receive Filter One Match is

0x(nil)

Press return for current value or enter new value: 0x0000a200000c

Receive Filter Two Type Options

1: Capture

3: Not Used

```
Current value for Receive Filter Two Type is 3
Press return for current value or enter new value:

Packet Capture Transmit Capture Filter Configuration
-----

Transmit Filter One Type Options
-----
1: Capture

3: Not Used
Current value for Transmit Filter One Type is 3
Press return for current value or enter new value:
```

Using the Load Subcommand

config packet load [*<slot>*] loads the Packet Capture utility on the specified slot.

<slot> specifies the slot number for loading Packet Capture. You can enter the slot number on the command line or have the script prompt you for it.

The following is a sample display of the **config packet load** command:

```
Performing mount check...

Enter slot number to load Packet Capture: 5
```

Using the Unload Subcommand

config packet unload [*<slot>*] unloads the Packet Capture utility on the specified slot.

<slot> specifies the slot number for unloading Packet Capture. You can enter the slot number on the command line or have the script prompt you for it.

The following is a sample display of the **config packet unload** command:

```
Performing mount check...

Enter slot number to unload Packet Capture: 5
```


Symbols

*, in get command, 1-17

A

ACE32 memory limitations, 3-13

adding VC gate w/GH event message, 5-6

address format, synchronous, 5-24

adjacency control blocks, 6-22

adjacency ID, 6-23

AFN memory limitations, 3-13

aggregate cell rate, 5-3

alignment error, 5-11

alternate mark inversion (AMI), A-36

alternating MAC addresses, 6-11

AMI. *See* alternate mark inversion

AN memory limitations, 3-13

AppleTalk, 6-2 to 6-4

ARN router, Packet Capture note, B-4

arp -a command, 7-9

ARP cache, 6-11, 7-9

ASCII files

 saving tables, 1-22

 saving the log, 1-6

ASN

 cables, 3-5

 slot ID, 3-5

 SPEX net module, 3-4

asterisk, in get command, 1-17

asynchronous file transfers to Bay Networks, 8-3

ATM, 5-2 to 5-6

ATM_ERR codes, 5-6

LANE, 5-7

 maximum number of virtual circuits (VCs),
 5-3

 Packet Capture, B-52

 SAR frame errors, 5-3

 VC mod failed message, 5-5

 virtual channel link (VCL) configuration, 5-3

attributes, 1-10 to 1-18

B

B8ZS (binary 8 zero substitution), A-37

babbling transmitter errors, 5-11

BablErrorTx, 5-11

backing up files, 1-3

bad forward receive buffer checksum errors, 3-17

base line number, B-8

base records, 1-2, 6-30

Basic Rate Interface (BRI) digital subscriber
 loops (DSLs), 6-28

Bay Networks anonymous FTP file server, 8-3

Bay Networks Press, xxii

BCN circuit breaker, 3-2

bipolar violations, A-37

bisynchronous, Packet Capture, B-9, B-53

blown fuse, 3-2

BofL. *See* Breath of Life errors

boot

 failure, 3-3

 image. *See* router software image

- PROMs, 3-6
- bouncing MAC addresses, 6-11
- Breath of Life (BofL) errors, 3-17
- bridge ID, 6-4
- buffers
 - allocating for Packet Capture, B-11
 - memory allocation error, 3-12

C

- cables, 4-3
- call request number (CRN), 6-23
- cannot find file message, 7-2
- carrier loss, 5-11
- case sensitivity, 1-16
- cells, 5-3
- Chameleon, 7-2
- CHAP (Challenge Handshake Authentication Protocol), 6-29
- check sequence (checksum) error, 5-11
- circuit breaker, 3-2
- circuit down, 5-17
- clearlog command, 1-5
- clipped (dropped) frames, 5-13
- clock settings, internal, 5-26
- clock speed does not match other ports event message, 5-26
- clocking, MCT1, 5-21
- CN circuit breaker, 3-2
- commands
 - arp -a, 7-9
 - clearlog, 1-5
 - commit, 1-3, 1-16
 - diags, 3-20
 - get, 1-16, 8-4
 - get command wildcard character (*), 1-17
 - ifconfig -a, 7-9
 - list, 1-13 to 1-17
 - loadmap, 3-14 to 3-16

- log, 1-7
- monitor, 1-18
- netstat -r, 6-8
- osidata, 6-21
- ping, 1-20
- pktconv, B-37
- pktdump, B-14, B-35
- prom command failed, 1-4
- put, 8-4
- run setpath, 1-18
- save config, 1-3
- save log, 1-5
- set, 1-2, 1-3, 1-16
- show, 1-18
- wfchkenv, 7-3
- wfchkinst, 7-4
- commit command, 1-2, 1-3, 1-16
- config packet command, C-1 to C-5
- configuration files, consistency among slots, 3-9
- Configuration Manager modes, 1-2
- configuration, saving, 1-16
- contiguous free space, 3-12
- converting Packet Capture files, B-36
- Create attribute, 6-30
- crossover cables, 5-26
- CSMA/CD. *See* Ethernet
- Current Screens List window, 1-19
- customer support
 - programs, xxiii
 - Technical Solutions Centers, xxiii

D

- date and time, filtering events, 1-7
- debug event messages, 1-7, A-1 to A-35
- Default zone message, AppleTalk, 6-3
- Delete attribute, 6-30
- diags command, 3-20
- dial-on-demand Raise DTR event messages, A-18 to A-22

- dial-on-demand V.25bis event messages, A-23 to A-28
- digital signal, level 0 (DS0) channels, 5-20
- digital subscriber loops (DSLs), 6-28
- direct mode, 5-3
- direction, Packet Capture, B-18
- Disable attribute, 6-30
- displaying the event log, 1-5
- Distinct TCP/IP, 7-2
- DLCI/VC, 5-19
- DLSw (data link switching), 6-4 to 6-5
- downstream neighbor, 5-16
- dropped (clipped) frames, 5-13
- DS0 channels. *See* digital signal, level 0
- dynamic adjacency ID, 6-23
- dynamic mode, Configuration Manager, 1-2

E

- E1, Packet Capture, B-9
- echo requests, ICMP, 7-7
- election process, A-5
- Enable attribute, 6-30
- environment variables, 7-3
- ESF. *See* extended super frame
- Ethernet, 5-9 to 5-14
 - heartbeat test (SQE), 5-13
 - memory errors, 5-12
 - Packet Capture, B-9, B-51
 - QENET, 5-13
- event messages
 - dial-on-demand Raise DTR, A-18 to A-22
 - dial-on-demand V.25bis, A-23 to A-28
 - MCT1, A-29 to A-37
 - sending to Bay Networks, 8-3
 - system startup, A-2 to A-17
- Events Manager tool, 1-5
- explicit addressing, 5-24, 5-25

- extended super frame (ESF), A-36

F

- facility data link (FDL) Disable Payload option, A-31
- fail LED, 4-4
- fault event messages, 1-7, 1-9, 3-20
- faxing copies to Bay Networks, 8-3
- FDDI, 5-14 to 5-16
 - cable colors, 4-5
 - Packet Capture, B-9, B-56
 - ports, loopback testing on, 4-5
- FDDI System Interface (FSI), 5-14
- fiber colors, 4-5
- file names, Packet Capture, B-32
- file was inaccessible message, 7-4
- filtering
 - event messages, 1-6 to 1-8
 - packets with Packet Capture, B-21 to B-27, B-46 to B-51
- format of an instance, 1-15
- forwarding tables
 - memory shortage, 3-13
 - saving, 1-22
- frame check sequence (FCS), B-4
- Frame Relay, 5-17 to 5-19
 - Packet Capture, B-53
- frames clipped (dropped), 5-13
- free space, 3-12
- FRE-II memory limitations, 3-13
- FTP
 - file server, Bay Networks, 8-3
 - memory-card error, 3-11
 - Packet Capture files, B-32
 - troubleshooting, 6-8 to 6-9
- fuse, blown, 3-2

G

GAME forward (GFWD) message type, A-5
GAME remote procedure call (GRPC) message type, A-5
GAME. *See* Gate Access Management Entity
Gate Access Management Entity (GAME), 1-9
gates, 1-9
get command, 1-16, 1-17, 8-4
global
 memory, 3-12
 parameters, 1-2
 SRB settings, 6-4
group LAN ID, 6-4
group mode, 5-3, 5-19

H

heartbeat test, Ethernet, 5-13
help from the Bay Networks Technical Solutions Center, xxiii, 8-1
host did not respond message, 6-12
HOST/ARP cache, 6-11
hot-swapping
 and fuses, 3-2
 cable support for, 4-4
HPTP, Packet Capture, B-36
HSSI
 connector state values, 4-2
 Packet Capture, B-10, B-36, B-56
hybrid mode, 5-3

I

ICMP echo requests, 7-7
ifconfig -a command, 7-9
image names. *See* router software image names
 or boot PROMs
implementation notes, Packet Capture, B-4

inbound Telnet. *See* Telnet
index of a logical line, B-8
informational events, 1-7
instance, 1-10 to 1-18
 creating for Packet Capture, B-7
 deleting for Packet Capture, B-17
 format, 1-15
Inter Frame Time Fill parameter, 5-21
interface definition, 7-9
internal clock settings, 5-26
internal clocking, MCT1, 5-21
internal LAN ID, 6-4
internal overrun errors, 5-14
invalid ID, can't parse cmd line message, 6-22
invalid slot number, can't parse cmd line message, 6-22
IP, 6-6 to 6-16
IP addresses, UNIX, 7-9
IPX, 6-16 to 6-20
IPX (RIP Supply and RIP Listen), 6-18
ISDN B channel, Packet Capture, B-9, B-10, B-57
ISDN BRI and PRI, 6-27 to 6-29

K

killing a gate, 1-9

L

lack-of-resource errors, 5-11, 5-15
LAN ID, 6-4
LAPB. *See* Link Access Procedure-Balanced
late collisions, 5-14
Launch Facility tool, 1-19
LEDs
 failure to light, 3-3
 power supplies, 3-2
 red fail, 4-4

- line build out (LBO), MCT1, 5-21
- line coding, 5-20
- line number, B-7, B-8, B-43, B-57
- Line Tests option, MCT1, A-29
- line type, 5-20, A-36
- Link Access Procedure-Balanced (LAPB), Packet Capture, B-53
- link state database, 6-15
- link state packets (LSPs), 6-22
- list command, 1-13 to 1-17
- load command, Packet Capture, C-5
- loadmap command, 3-14
- local
 - loopback test, 4-4, 5-24
 - memory, 3-12 to 3-16
 - mode, Configuration Manager, 1-2
 - network range conflict, 6-3
- log
 - AppleTalk filter, 6-2
 - ATM filter, 5-2, 5-7
 - command, 1-7
 - CSMA/CD (Ethernet) filter, 5-9
 - data link protocol filter, 5-29
 - DLSw filter, 6-4
 - FDDI filter, 5-14
 - filtering, 1-6 to 1-8
 - Frame Relay filter, 5-17
 - FTP filter, 6-8
 - IP filter, 6-6
 - IPX filter, 6-16
 - MCT1 filter, 5-20
 - modem interface filter, 6-23
 - network layer protocol filter, 6-30
 - OSI filter, 6-21
 - OSPF filter, 6-15
 - PPP filter, 6-23
 - saving to an ASCII file, 1-6
 - switched services, 6-24, 6-28
 - synchronous filter, 5-22
 - Telnet filter, 6-8
 - TFTP filter, 6-8

- token ring filter, 5-27
- logical line number, B-8
- logical link control (LLC) reception ring
 - overruns, 5-15
- loopback test, 4-4, 5-24
- loss-of-carrier errors, 5-11
- lost password, 3-10

M

- MAC addresses
 - alternating, 6-11
 - source, 5-28
- master cannot connect to slave, dial backup, 6-25
- maximum transmission unit (MTU), ATM, 5-3
- MCT1, 5-20 to 5-21
 - creating a Packet Capture instance, B-7
 - event messages, A-29 to A-37
 - Inter Frame Time Fill parameter, 5-21
 - internal clocking, 5-21
 - LBO, 5-21
 - Line Tests option, A-29
 - super frame (SF), A-36
- mct1el.exe file, 5-21
- media-specific state, 4-1
- memalloc (memory allocation) event message, 3-12
- memory, 3-12
 - allocating for Packet Capture, B-11
 - allocation error, 3-12
 - available space, 3-12
 - card, space shortage, 3-11
 - errors, Ethernet, 5-12
- MIB
 - accessing via Technician Interface commands, 1-16
 - Quick Get tool, 1-19
 - retrieving values, 1-19
 - specification, 1-14 to 1-15
 - structure, 1-10

modem, using to transfer files to Bay Networks,
8-3

monitor script commands, 1-18

multimode fiber, orange, 4-5

munich.exe file, 5-21

N

netstat -r command, 6-8

Network General Sniffer

- converting a Packet Capture file for, B-36
- format, 1-20

network unreachable message, 1-20, 6-8, 6-12

no answer from called slot message, 6-22

no data returned for ID message, 6-22

non-word-aligned frames, 5-13

Number of Zones on Extended Net Conflict event
message, 6-3

O

object does not exist message, 1-17

objects, 1-10 to 1-18

orange fiber, 4-5

OSI, 6-21 to 6-23

osidata command, 6-21

out of resources error, 3-12

P

Packet Capture

- ARN note, B-4
- ATM, B-52
- bisynchronous, B-53
- configuring, C-1
- converting files, B-36
- CSMA/CD, B-51
- deleting an instance, B-17
- direction, B-18
- displaying
 - configuration settings, B-30

- using a Sun workstation or DOS PC, B-35
- using the Technician Interface, B-14

enabling, B-12

event messages, B-31

FDDI, B-56

file names, B-32

filtering, B-21 to B-27, B-46 to B-51

Frame Relay, B-53

getting a file, B-32 to B-35

HSSI (high-speed serial interface), B-56

implementation notes, B-4

instance, B-7, B-57

introduction, 1-20

ISDN, B-57

LAPB, B-53

listing attributes, B-38

overview, B-2

parameters

- Buffer Size, B-43

- Capture, B-42

- Control, B-42

- Count, B-44

- Delete, B-40

- Direction, B-44

- Disable, B-41

- Filename, B-42

- Filter Size, B-25

- Group, B-21, B-26, B-51

- Line Number, B-43, B-57

- Match (string), B-21, B-23, B-50

- Offset, B-21, B-25, B-48

- Packet Size, B-12, B-44

- Receive Filters, B-21

- Reference, B-21, B-24, B-49

- Size, B-21, B-50

- State, B-41

- Transmit Filters, B-21

- Trigger, B-45

- Type, B-21, B-22, B-47

Passthru, B-54

pktconv command, B-37

PPP, B-54

SDLC, B-55

SMDS, B-55

- starting, B-13
- terminating, B-13
- token ring, B-56
- trigger, B-19
- X.25, B-55
- parameters. *See* attributes
- Passthru, Packet Capture, B-54
- Password Authentication Protocol (PAP), 6-29
- password lost, 3-10
- path control blocks, 6-22
- path is invalid message, 7-3
- path variables, 7-3
- payload loopback, A-29, A-31
- permanent virtual circuit (PVC), not receiving, 5-18
- ping command
 - failure of, 6-9, 7-9
 - using, 1-20
- pktconv command, B-37
- pktdump command, B-14, B-35
- Point-to-Point Protocol (PPP)
 - Bay Networks Proprietary, B-54
 - lines, loopback testing on, 4-4
 - Standard, B-54
- power problem, 3-2
- power surge, 3-2
- processors, configuring for Packet Capture, B-5
- Procom file transfers to Bay Networks, 8-3
- program counter (PC), 3-14
- prom command failure, 1-4
- PROM image compatibility, 3-6
- Proxy ARP, 6-13
- publications, Bay Networks, xxii
- put command, 8-4

Q

- Quad Ethernet (QENET), 5-13

- Quick Get tool, 1-19

R

- Raise DTR dial services
 - RS-232, 6-25
 - V.35, 6-26
- receiver lack-of-resource errors, 5-11
- reception statistics not changing, 5-29, 6-31
- red fail LED, 4-4
- reliable message types, A-5
- remote loopback test, 4-4, 5-25
- remote mode, Configuration Manager, 1-2
- Reset button, 3-20
- retrieving files from Bay Networks, 8-3
- RIP
 - IP, 6-14
 - IPX, 6-18
- RIP Supply and RIP Listen, IPX, 6-18
- router software image
 - consistency among slots, 3-7
 - names, 3-6
- routing tables, 1-22
 - displaying on UNIX, 6-8
 - memory shortage, 3-13
- RS-232 Raise DTR dial services, 6-25
- run setpath command, 1-18

S

- save config command, 1-3, 1-16
- saving
 - configuration changes, 1-3
 - forwarding tables, 1-22
 - memory-card files, 3-11
 - output to disk option, 1-6
 - routing tables, 1-22
 - the log, 1-5
- scope of a problem, determining, 2-1 to 2-3
- Screen Builder tool, 1-19

- Screen Manager tool, 1-19
- script commands, 1-18
- SDLC, Packet Capture, B-55
- secret, CHAP, 6-29
- Seed Conflict message, AppleTalk, 6-3
- segmentation and reassembly (SAR) frame errors, 5-3
- sending files to Bay Networks, 8-3
- serial number, getting, 8-2
- Service Profile Identifiers (SPIDs), 6-28
- SERVICES file, 7-3
- set command, 1-2, 1-3, 1-16
- severity of events, 1-7
- show script commands, 1-18
- signal quality error (SQE) test, 5-13
- single-mode fiber, yellow, 4-5
- Site Manager, 7-1 to 7-9
- slot
 - configuring for Packet Capture, B-5
 - mask, B-5
- slot, ASN
 - dial, 3-5
- SMDS, Packet Capture, B-55
- SNMP, 7-5 to 7-6
- SNMP MIB could not be loaded from the file message, 7-4
- soloist, A-5
- space shortage
 - on memory card, 3-11
 - on transmission (Tx) queue, 5-12
- Stack Packet Exchange (SPEX) net module, 3-4
- startup event messages, A-2 to A-17
- State attribute, 6-30
- static configuration conflict event message, 6-4
- Statistics Manager tools, 1-19
- statistics not changing, 5-29, 6-31
- subnet mask, 6-13

- UNIX, 7-9
- super frame (SF), MCT1, A-36
- switched services, 6-23 to 6-29
- synchronous connections, 5-22 to 5-26
 - Packet Capture, B-9
- system startup event messages, A-2 to A-17

T

- T1, Packet Capture, B-9
- target does not respond message, 1-20
- TCP connection state
 - enabling, 1-21
 - verifying, 6-5
- TCP/IP communication stack, 7-2
- Technical Solutions Centers, xxiii
- Technician Interface, 1-10
 - See also* commands *and* Telnet
- Telnet, 1-21
 - enabling, 1-21
 - troubleshooting, 6-8 to 6-9
- termination trigger
 - Packet Capture, B-45
- termination trigger, Packet Capture, B-19
- terminator plugs, inserting in SPEX module, 3-5
- TFTP, 6-8 to 6-9
 - memory-card error, 3-11
 - Packet Capture files, B-33
- TFTP file transfers to Bay Networks, 8-3
- time, filtering events, 1-7
- token ring
 - Packet Capture, B-9, B-56
 - troubleshooting data link layer, 5-27
 - troubleshooting physical medium, 4-2
- tools
 - Launch Facility, 1-19
 - Quick Get, 1-19
 - Screen Builder, 1-19
 - Screen Manager, 1-19
 - Statistics Manager, 1-19

See also Packet Capture

trace events, 1-7

transmission (Tx) queue space shortage, 5-12

transmission statistics not changing, 5-29, 6-31

trigger, termination, B-19, B-45

U

UDP port numbers for SNMP, 7-3

unable to find UDP port numbers for SNMP message, 7-3

unable to load the SNMP MIB message, 7-4

unable to run . . . module message, 7-4

unaligned frames, 5-13

underflow errors, 5-22, 5-23

unknown database object type, can't parse cmd line message, 6-22

unknown network message, 1-20, 6-8

unload command, Packet Capture, C-5

upstream neighbor, 5-16

User Screens window, 1-19

V

V.25bis, 6-23

V.35 Raise DTR dial services, 6-26

values, 1-10

variables. *See* attributes

VC ATM add mod failed message, 5-5

virtual channel link (VCL) configuration, 5-3

virtual circuits (VCs), maximum number of ATM, 5-3

virtual ring ID, 6-5

W

w/GH (with gate handle), 5-6

warning events, 1-7

wfAppleBase, 6-2

wfAtmAlcCopDataPath, 5-4

wfBisyncLineNumber, B-9

wfchkenv command, 7-3

wfchkinst command, 7-4

wfCSMACDEntry, 5-9

wfCSMACDLineNumber, B-9

wfDlsInterfaceEntry, 6-5

wfDs1E1PortMapLineNumber, B-8

wfFddiEntry, 5-14

wffddiLineNumber, B-9

wfFddiMacEntry, 5-16

wfHssiLineNumber, B-10

wfHwActiveImageName, 3-7

wfHwBase, 8-2

wfHwBootPromSource, 3-6

wfHwBpSerialNumber, 8-2

wfHwConfigFile, 3-9

wfIpBase, 6-6

wfIpBaseRtEntry, 6-15

wfIpInterfaceEntry, 7-9

wfIpNetToMediaEntry, 6-11

wfIsdnBriLineNumber, B-10

wfKernelBufOwnerTask, 3-14, 3-15

wfKernelEntry, 5-15

wfKernelMemoryMaxSegFree, B-11

wfKernParamEntry, 3-13

wfLogicalLineNumber, B-8

wfMCT1E1Load, 5-20

wfMunichLoad, 5-20

wfOspfBase, 6-15

wfOspfIfEntry, 6-16

wfPktCapture<Rx / Tx>Fltr<no.>Match, B-23, B-50

wfPktCapture<Rx / Tx>Fltr<no.>Offset, B-25, B-47, B-48

wfPktCapture<Rx / Tx>Fltr<no.>Ref, B-24,
B-49
wfPktCapture<Rx / Tx>Fltr<no.>Size, B-25,
B-50
wfPktCapture<Rx / Tx>Fltr<no.>Type, B-22
wfPktCapture<Rx / Tx>Fltr2Group, B-26, B-51
wfPktCapture<Rx / Tx>Trigger, B-19, B-45
wfPktCaptureBufSize, B-11, B-43
wfPktCaptureCapture, B-42
wfPktCaptureControl, B-13, B-42
wfPktCaptureCount, B-44
wfPktCaptureDelete, B-8, B-10, B-17, B-40
wfPktCaptureDirection, B-18, B-44
wfPktCaptureDisable, B-12, B-41
wfPktCaptureEntry, B-38
wfPktCaptureFname, B-42
wfPktCaptureLineNumber, B-43
wfPktCaptureLoad, B-5
wfPktCapturePktSize, B-12, B-44
wfPktCaptureState, B-41
wfPppWhoamiEntry, 6-29
WFSM.EXE, cannot find file message, 7-2
wfSwservOptsEntry, 6-29
wfSyncEntry, 5-22
wfTcpConnEntry, 6-5
wfTokenRingEntry, 5-28
wfTokenRingLineNumber, B-9
WINSOCK.DLL, cannot find file message, 7-2
working directory is invalid message, 7-3

X

X.21, 5-24
X.25, Packet Capture, B-55
XMODEM
transferring files to Bay Networks, 8-3

transferring Packet Capture files to a DOS PC
or a Sun workstation, B-35

Xoff state, 5-19

Y

yellow fiber, 4-5

YMODEM, Packet Capture, B-35

Z

Zone Name Conflict message, AppleTalk, 6-3